KPMG

cutting through complexity

INDIA FRAUD SURVEY 2012

TABLE OF CONTENTS

INTRODUCTION

India has been amongst the fastest growing economies in the world in the last decade. It has remained relatively unaffected by the global economic crisis, thanks to strong fundamentals of the economic policy. However, despite this situation the confidence of international investors and domestic entrepreneurs has been low in the last two years, thanks to the various scams that have come to light during this period. The need for improving governance and ethical culture across public and private sector companies has never been felt as acutely as is being felt now. This resounding sentiment is echoed in the KPMG India Fraud Survey 2012.

While there is greater awareness of fraud and misconduct among corporate India, the associated risks need to be considered at a strategic level. Investments need to be prioritised to build a sustainable ecosystem that can mitigate frauds efficiently, including frauds of the future. The KPMG India Fraud Survey 2012 has highlighted the emergence of newer forms of fraud and reliance on technology to perpetrate them. Cyber crime, Intellectual property (IP) fraud, piracy and counterfeiting, and identity theft have been identified as the key fraud risks of the future. Many respondents were aware of these frauds but had limited knowledge of the ways in which these frauds manifest themselves or how organisations could tackle them.

With the sophistication of fraud, companies need to take a long term view of fraud risk management and adopt comprehensive frameworks to mitigate fraud. As organisations strive to create a high performance culture, they must back these efforts by creating strong controls, pro-active supervision through use of technology and independent monitoring of key performance parameters to create deterrence for misbehavior.

While one cannot deny the challenges in fraud prevention and detection from external factors such as regulation/ law enforcement, one should realise that change comes from within. Some companies have demonstrated this by showing that business can be done in India ethically.

We wish to thank all our survey respondents who took time to respond to the survey and helped us derive the corporate sentiment on emerging frauds. Your views will help the industry in understanding the fraud landscape we face. We hope all of you find the survey interesting and thought provoking. Do let us know your views by writing to us or our colleagues.

DEEPANKAR SANWALKA
Partner and Head
Risk Consulting
KPMG in India

DINESH ANAND
Partner and Head
Forensic services
KPMG in India

FOREWORD

The global economy has faced considerable headwinds ever since the sub-prime crisis in US lead to the downfall of several large and well established enterprises. The resultant economic uncertainty, frailty of sovereign finances, volatile commodity prices, rising unemployment and falling consumer demand have created unparalled pressure on corporate performance across the globe. These crises have exposed the weaknesses of the governance structures at some of the major corporations which were until then considered progressive. One of the key fallouts of this situation has been the refinement of what corporates have considered 'acceptable behavior' in conducting business.

While the recently reported high profile incidents of frauds across the globe indicate the depth to which the malaise of fraud and corruption has spread, the relatively swift action by regulators and governments indicates the willingness to take action against the wrong-doers. While the enforcement action in India is not swift and decisive enough in comparison to our global counterparts, we are still striving to make that change and small steps in that direction have already been taken. The developed nations themselves took over two to three decades to reach the state of stringent enforcement currently prevalent in those geographies. India cannot afford to take a similar time to improve its enforcement and shall need to move much more swiftly towards stringent enforcement. This is imperative as India has a key role to play in the global economic revival and any disruption in the Indian economic growth is likely to have a global impact.

In this context, there is little doubt that even the fraud landscape is undergoing a considerable change with both incidences and magnitude of frauds witnessing a marked increase. Increasingly, frauds are becoming all pervasive – encompassing multiple locations, involving various stakeholders with increasingly complicated modus operandi adopted by the perpetrators. Corporates now have increased responsibility to fight this rising menace and improve the governance structure and ethical standards in business practices. Thus, reports/ surveys such as this one can help companies bridge any gaps in their governance and risk management frameworks.

Time and again, KPMG has led the way and highlighted some of the best practices that should be adopted to mitigate fraudulent activities. The KPMG India Fraud Survey report 2012 discusses corporate fraud at a macro/regulatory level as well as a micro/ control environment level. It highlights the urgent need for action on both these fronts and suggests actionable measures that can greatly help regulatory bodies and corporate leaders to fight the fraud menace and enhance India's investment attractiveness.

Key Findings

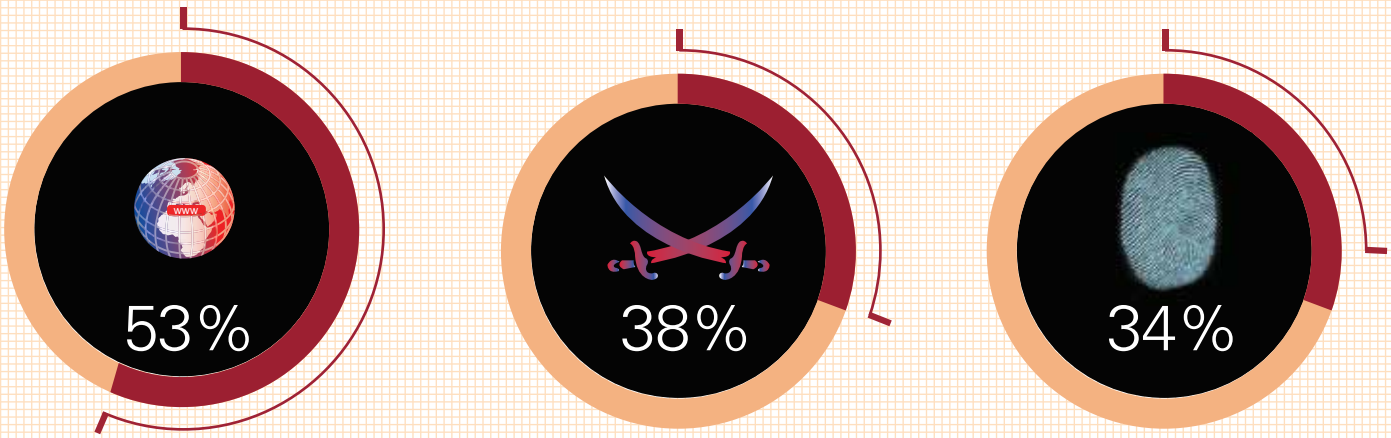
FRAUD AWARENESS

55% RESPONDENTS **EXPERIENCED FRAUD**

94% RESPONDENTS BELIEVE **FRAUDS HAVE BECOME MORE SOPHISTICATED**

71% RESPONDENTS BELIEVE **FRAUDS IS AN INEVITABLE COST OF DOING BUSINESS**

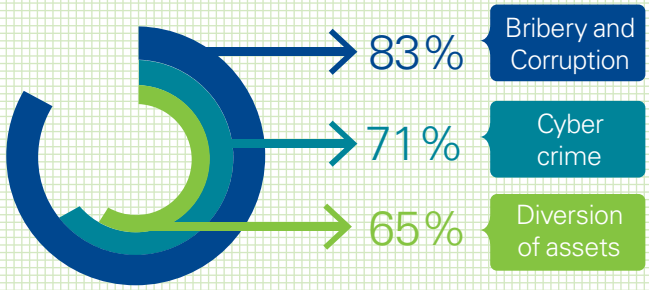
EMERGING FRAUDS ARE



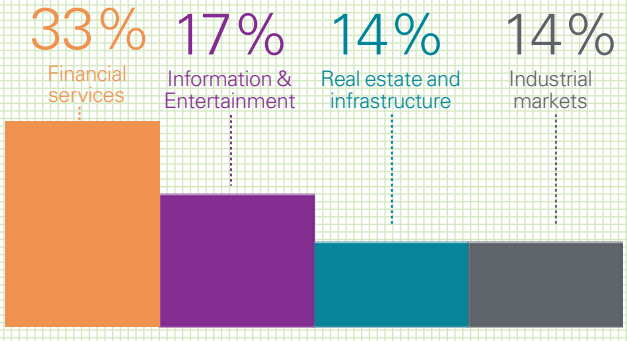
- Cyber crime
- IP theft, Counterfeiting and piracy
- Identity theft

INCIDENCE OF FRAUD

Types of frauds heard/ experienced

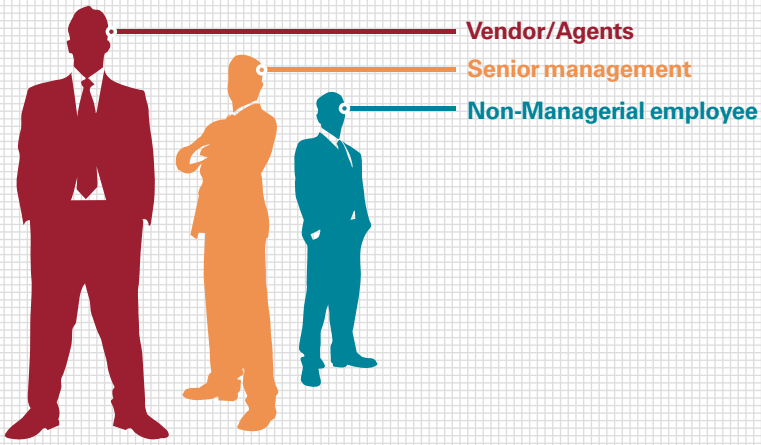


Sectors affected

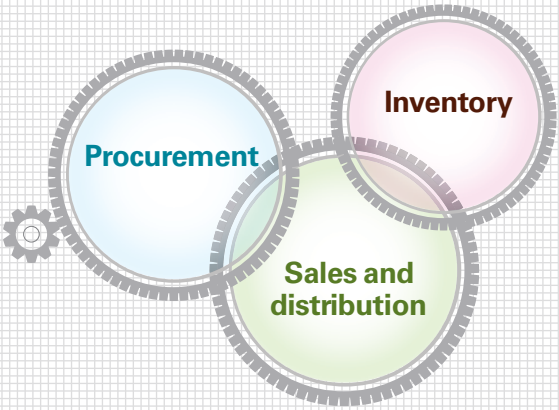


Source – KPMG India Fraud Survey 2012

People most susceptible to commit fraud

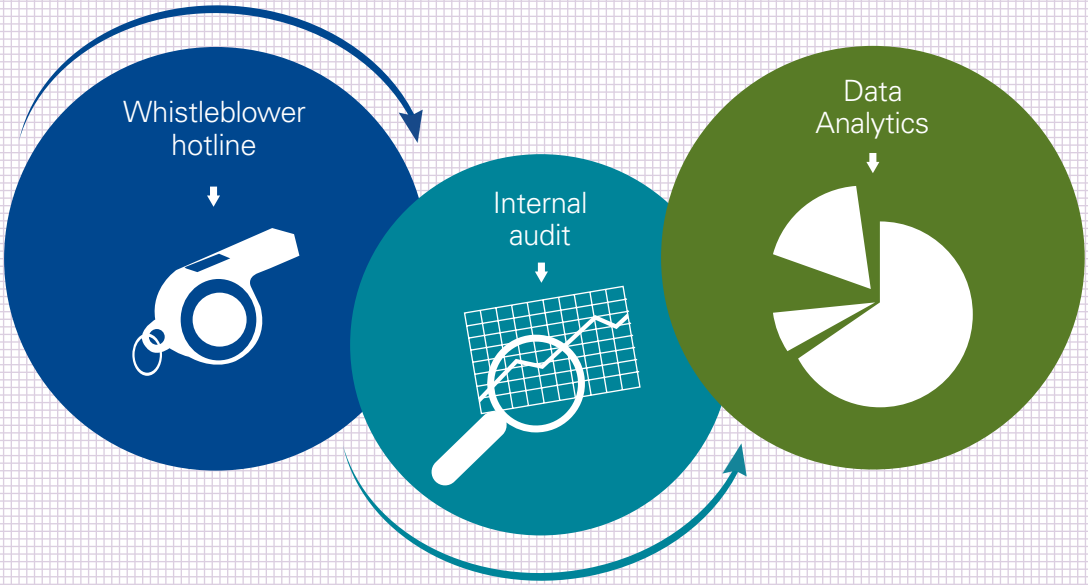


Processes most vulnerable to fraud



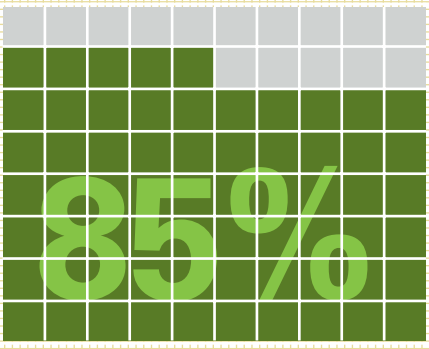
FRAUD DETECTION AND RESPONSE

Most effective ways to detect fraud

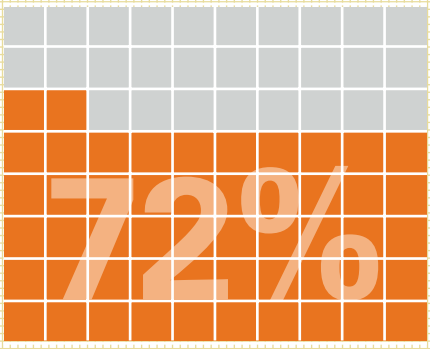


Response to fraud

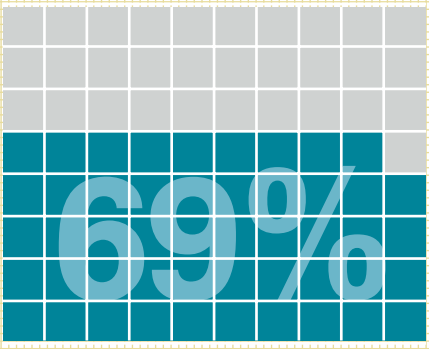
85% Internal Investigation



72% Modification of controls



69% Disciplinary action



Source – KPMG India Fraud Survey 2012

Section

01

At their wits' end - organisations overwhelmed tackling fraud

The last few years have seen increased number of frauds reported in India as well as globally, which upon observation, highlight a growth in the sophistication and scale of fraud. With reports indicating that as much as 5 percent of annual revenues could be lost to fraud[1], organisations today are required to be more cognizant of the damage that fraud can do.

The sheer magnitude and complexity of publicly reported frauds clearly indicates that more organisations appear to be succumbing to the pressure of performing in an increasingly uncertain global economic environment alongside growing stakeholder expectations. The rising cost pressures, changing risk perceptions and regulatory activism is redefining the contours of acceptable ethical behavior.

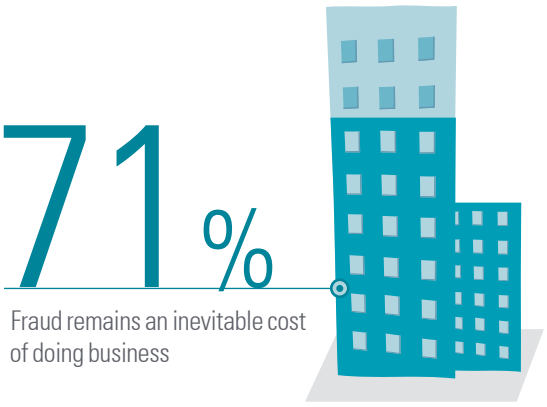
Our fraud survey echoes some of these sentiments and also provides insights into some of the newer experiences of fraud witnessed by some of the organisations in corporate India. As we see the emergence of this newer face of fraud, corporate India continues grappling to fight the rising menace.

1 2012 ACFE Global Fraud Study, "Report to the Nations on Occupational Fraud and Abuse"

Corporate India dubs rising fraud as 'inevitable cost of business'

Notwithstanding the number of media reports on fraud, the last two years have seen a substantial increase in the incidence of fraud. Close to 55 percent of respondents indicated that their organisations experienced fraud in the last two years vis-à-vis 45 percent in the 2010 edition of our fraud survey.

This increase can be attributed to several aspects. The ongoing economic slowdown for one puts pressure on individuals to perform and tempts them to commit fraud. It is also in a downturn that frauds are most likely to be discovered (even though perpetrated much earlier), as that is when managements increase their scrutiny in a bid to protect margins and profits. Thirdly, greater awareness of fraud and its impact can result in companies becoming more sensitive to noticing frauds, which otherwise tend to go unnoticed or are deliberately overlooked.



However, it is surprising to note that 71 percent of the respondents think of fraud as an inevitable cost of doing business.

This includes 80 percent of respondents who stated that they had experienced fraud in the last two years. Indian companies outnumbered multinational firms in this view.

This is dangerous as it could lead to organisations having a tolerant approach towards fraud and subsequently not investing enough in the appropriate fraud risk management controls and framework. It also translates into a culture of merely reacting to fraud and not proactively taking steps to mitigate it.

In such a scenario the onus would be on regulatory bodies to ensure that firms follow a robust fraud risk management framework, failing which they would face stringent action. This has been the case with most regulated industries such as financial services.

Fraud becoming more sophisticated

Please refer to **"Section 2: Bribery and Corruption – Corporate India reluctant to tackle bribery and corruption"** on **page 19** for further details

Our survey responses indicate that bribery and corruption (83 percent) is perceived to be a major concern followed by e-commerce & other cyber related frauds (71 percent) and diversion/theft of funds or goods (65 percent). The findings differ from our previous survey where diversion/theft of funds or goods was identified as the most common fraud followed by bribery and corruption and cyber related frauds.

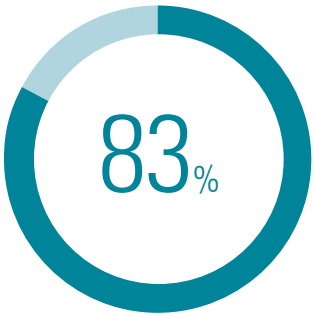
Please refer to **"Section 3A: Cyber Crime – silently permeating through organisations"** on **page 37** for further details

In today's day and age technology has become a mainstay for all industries, irrespective of sector or size. Our experience indicates that even fraudsters are becoming technology savvy and are finding newer ways of perpetrating frauds. In the past, technology driven frauds were reported to have much lower incidence compared to frauds of a conventional nature such as diversion/ theft of goods. However, today there is increased awareness about technology led frauds.

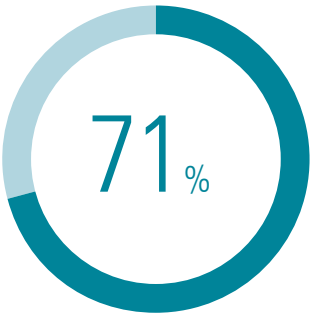
This awareness can be attributed to the increased media coverage of such frauds. A case in point is the recently unearthed sophisticated bank fraud that originated in Italy and spread globally, initiating the transfer of almost USD 78 million from around 60 financial institutions[2]. Perpetrators attacked the computers of wealthy individuals and carried out these fraudulent transactions from their bank accounts. These transactions were hidden by an additional layer of malware to delay discovery. The malware circumvented the two-stage authentication and other fraud prevention and detection methods employed by the banks. The manner in which the fraudsters had beaten the complex banking controls points towards the rising sophistication of fraud.

2 "Sophisticated bank fraud attempted to steal at least $78 million", Ars Technica, 27 June 2012

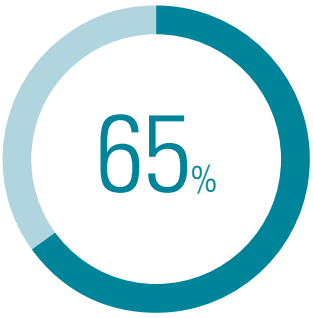
Types of frauds heard / read / experienced
(Multiple choice)



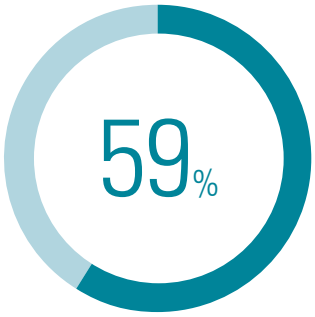
Bribery and Corruption
(including kickbacks)



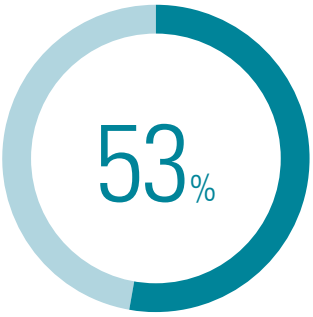
e-Commerce, internet and Cyber related fraud



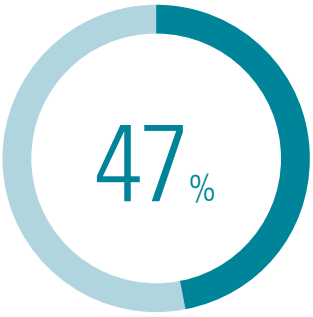
Diversion/theft of funds or goods
(through false invoicing, fake claims, pilferage)



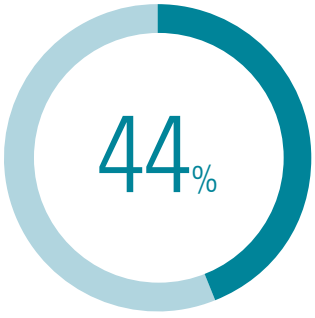
Financial statement fraud



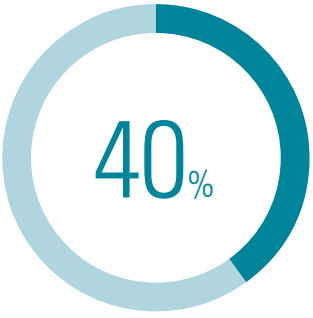
Regulatory non-compliance



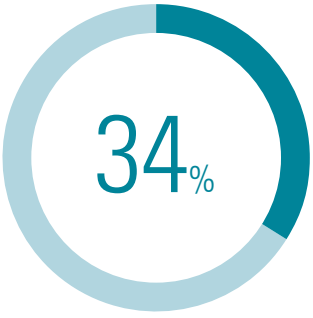
Money laundering



Internal reporting
(example: MIS reports related fraud)



Intellectual Property Fraud
(counterfeiting, piracy)



Others

Source – KPMG India Fraud Survey 2012

The perception levels for frauds like money laundering (47%), internal reporting related frauds (44%) and intellectual property fraud (40%) too are significantly higher (compared to our 2010 survey). These frauds today rely on technology to increase their impact.

For instance, money laundering is no longer a risk limited to the banking industry. Thanks to widespread misuse of technology to launder/ circulate money, sectors like insurance and mutual funds also provide conditions for such activities to be perpetrated. Consequently, regulators have extended anti-money laundering controls to cover insurance and mutual funds sectors. Recently, the Registrar of Companies was asked to probe the involvement of 13 companies in these sectors over allegations of money laundering and money circulation.

In case of intellectual property (IP) theft/fraud, technology is a convenient and inexpensive channel to execute fraud. A single email can transfer confidential IP to unauthorised parties without raising any suspicions or violating any internal controls. Theft or fraud of IP is extremely difficult to track as the original information remains on the computer of the creator. It is also difficult to indicate what truly constitutes IP as most of the data gathered is still in an early stage with unknown potential. In such a case, parts of the data can be easily obtained and sent to unauthorised parties such as competitors. What this can do is speed up the go-to-market strategy of a competitor.

Please refer to **'Section 3B: Rampant IP Fraud, Counterfeiting and Piracy in industry, yet corporates grapple to understand business impact'** on page **43** for further details

For many years now, MIS related frauds (internal reporting) have featured among the top five business concerns. With increased adoption of technology, although rudimentary controls are established, fraudsters can cleverly manipulate data such as sales commissions (mainly percentage figures), expenses (forged bills) and assets to ensure that results are consistent with expectations, while still siphoning off money.

Understanding the modus operandi of the frauds mentioned above and detecting them is not easy, and 94 percent of our respondents agreed that frauds had become sophisticated in the last two years. Investigators too are constantly challenged by the sophistication of frauds.

A case in point is the the Telecom industry that has had its share of losses due to sophisticated technology aided frauds. Globally, telecom frauds are estimated to cost the industry USD 40 billion,[3] despite significant efforts made by operators and their software/ hardware vendors to limit theft. Operators' billing systems and network vulnerabilities are always the key target areas for most fraudsters who exploit any weaknesses in these areas. We have successfully investigated multiple frauds by analysing data on social media where such information can often be found.

Thus, type of fraud and its degree of sophistication tend to be sectoral in nature. Certain technology intensive sectors such as financial services and IT or ITES are more vulnerable to cyber related frauds, whereas, sectors such as real estate and infrastructure are more prone to conventional frauds such as bribery and corruption and diversion of funds/ goods.

94%

Frauds have become more sophisticated in the last two years

3 Heavy Reading Service Provider IT Insider report

Financial services sector faces the maximum threat of fraud

Financial services and information and entertainment sectors have been identified as most vulnerable to fraud by respondents.

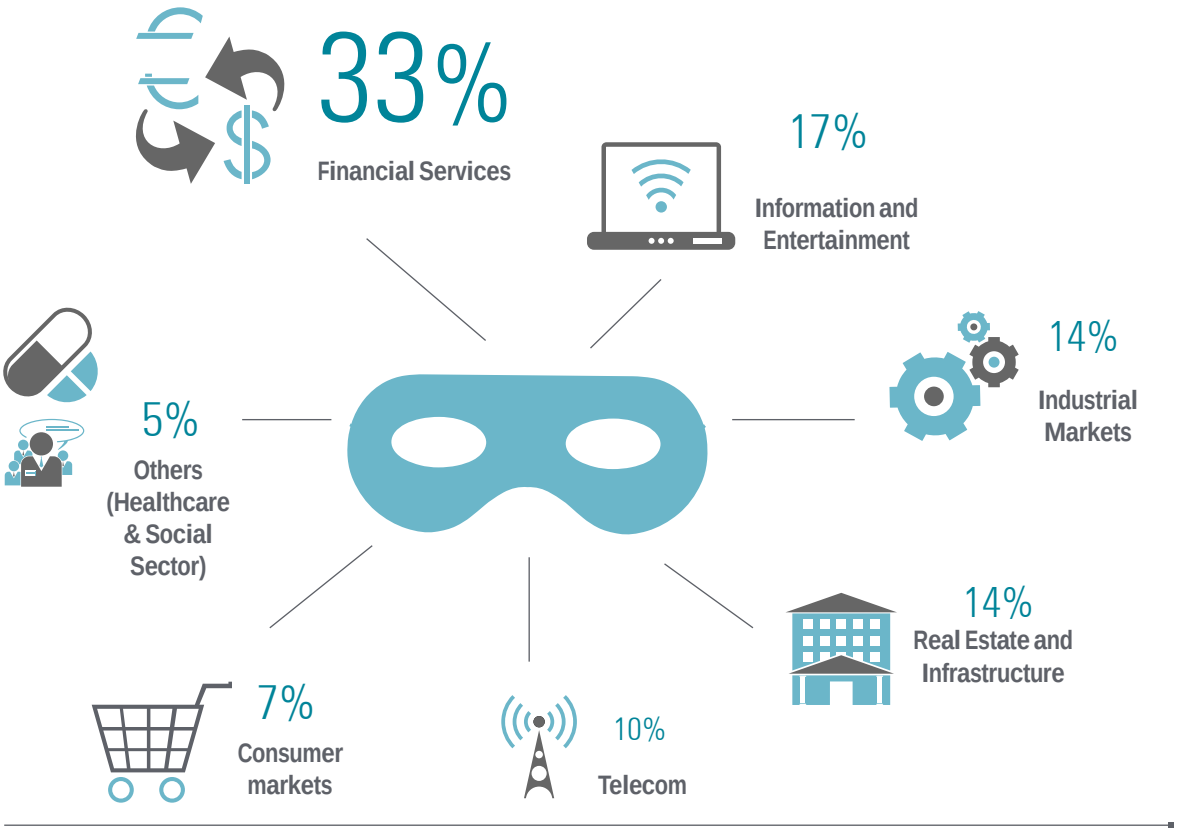
Interestingly, both sectors identified are heavy users of technology implying that while technology can be a great facilitator for the business, it can also offer an equally potent platform for committing frauds like cybercrime, phishing and data theft.

Despite having a strong regulator, the financial services sector has emerged as the most susceptible sector to fraud. Possible misuse of technology in the banking sector includes use of banking access for overpayments to vendors/ self bank account, sharing of potential confidential information and misuse of company's technology resources for unauthorised activities including conflicting business relationship. Additionally, providing services on mobile and social media platforms with limited knowledge of the security requirements, poses threats to customers as well as financial institutions.

In case of the information and entertainment sector, despite functioning as global entities and complying with stringent foreign legislations, they have been identified as the second most fraudulent sector in India. Thus, organisations need to be more proactive and adopt a zero tolerance approach towards fraud risk management

Please refer to **'Similar trends, yet different manifestations - Sector perspectives on emerging frauds in India'** on page **59** for further details

Sectors perceived as most vulnerable to fraud



Source – KPMG India Fraud Survey 2012

Procurement function continues to be most vulnerable to fraud

While incidences of newer types of frauds are on the rise, from a process perspective they continue to be targeted towards the same business processes. Not surprisingly, 72 percent of our survey respondents have agreed with such a perception. It is thus important to understand the operational characteristics of each sector to identify functions vulnerable at a sectoral level.

Our survey respondents have rated procurement, sales and distribution and inventory as the most vulnerable processes within an organisation. These areas being characterised by large number of stakeholders, multiple touch points, increasingly complex processes involving a significant proportion of organisations' funds, it is not surprising to see this finding. Additionally, these processes involve a high degree of interaction with external stakeholders like vendors and customers where collusion can override certain internal controls.

Despite the widespread acknowledgement of the vulnerability of these processes, organisations have failed to implement basic controls. Due diligence of vendors before selection, involvement of representatives from multiple departments in the vendor selection process, and adequate segregation of duties and controls over access rights, are some of the controls which may help organisations in managing these risks better.

Process perceived as most vulnerable to fraud risks
(Ranks are based on total score. Rank '1' indicates most vulnerable Process)

Procurement	01
Sales and Distribution	02
Inventory	03
Finance/Payments	04
Administration	05
Treasury	06
HR	07

Source – KPMG India Fraud Survey 2012

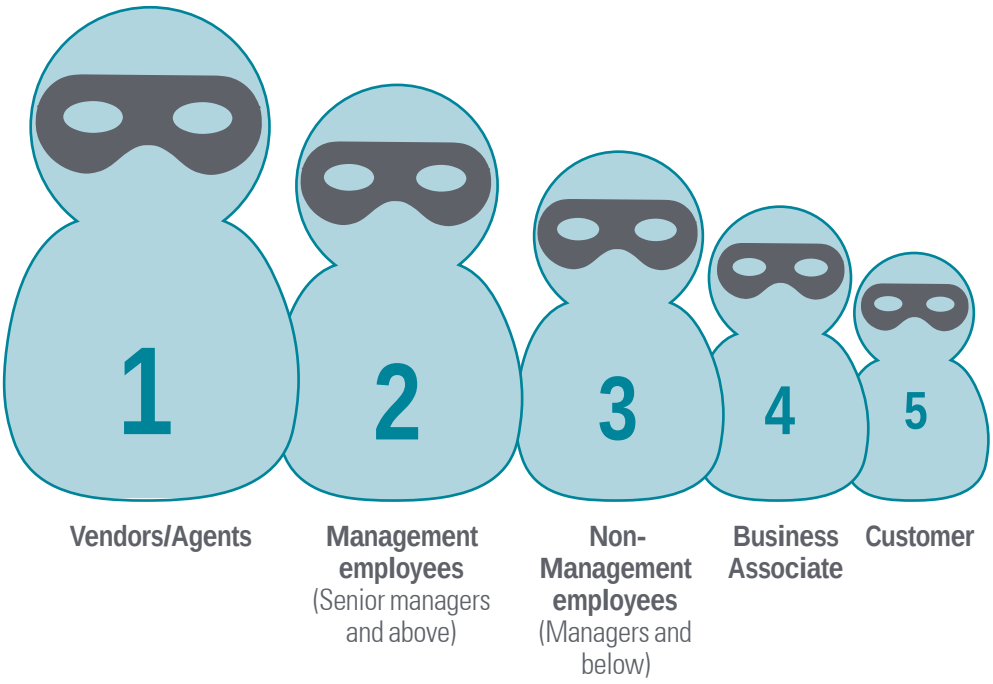
Companies undermine threat posed by the 'enemy within'

In our experience, employees are often central to frauds as they either perpetrate the fraud or assist an external team to do so. Hence, the larger threat of fraud lies within an organisation itself. However, most organisations tend to ignore or merely warn respective employees upon discovery of small value frauds (such as faking personal bills or fudging of expense reports). Therefore, when employees collude with external parties to commit fraud (such as processing fake invoices submitted by vendors), organisations often tend to blame external parties first and not employees. This could be a possible reason for our survey respondents to have ranked vendors/agents as the most likely to commit fraud against an organisation.

Among employees, senior management is considered the most susceptible to committing fraud by virtue of their ability to override existing controls. According to the ACFE 2012 Global Fraud Study, the position held by the fraudster within an organisation is directly related to the loss incurred on account of the fraud committed. Losses caused by senior management were approximately three times higher than the value of fraud loss due to managers; managers in turn caused losses approximately three times higher than junior employees.

In such circumstances it becomes imperative for organisations to provide a safe, robust channel for employees to report suspicions of malpractice. It is also important that an organisation's Board comprise of individuals with utmost integrity who would engage themselves with the management. The Board needs to take a lead by setting the tone at the top and facilitate a zero tolerance approach towards fraud.

Who is most susceptible to commit fraud?
(Ranks are based on total score. Rank '1' indicates most susceptible people)



Source – KPMG India Fraud Survey 2012

Employees more confident using whistle blower hotlines to report fraud

Numerous fraud surveys have indicated that internal stakeholders are highly susceptible to committing fraud. However, these surveys have also indicated that most frauds are unearthed from tips or complaints by sources internal to an organisation[4]. This fact is reiterated in our survey with respondents identifying whistleblower hotlines as the most effective way to detect fraud.

An effective mechanism providing comfort to the complainant that their identity would remain anonymous and that the information disclosed would be handled in a safe and confidential manner have resulted in a number of fraud related issues being reported on such channels. It has been observed that such hotlines also become preventive tools over a period of time.

Most multinational companies have whistleblower hot lines as mandated by regulators in their home countries. However, we have seen an increase in the number of Indian business houses opting for such hotlines. Both Indian and multinational companies are reviewing their business code of conduct, whistleblower policies and putting in place committees, rather than individuals, to receive such complaints and to act on them. Complaints received are tracked and the progress on each complaint is discussed in committee meetings.

The critical success factors for a whistleblower hotline include an independent, anonymous and confidential mechanism that is easy to access. This, backed by a well defined and structured committee empowered to act on complaints received can help build whistleblower confidence in the entire mechanism.

Besides whistleblower hotlines, survey respondents have also highlighted data analytics as one of the effective ways to detect fraud. Considering most companies today deal with vast and complex data, real time analytics and dashboard tools can be adopted to highlight any red-flags and capture any deviation from the routine, which could be an indication of a fraud. These tools are very effective in detecting fraud at an initial stage.

However, in our experience we have observed that, barring few organisations, not many make use of the data available to them on their Enterprise Resource Planning (ERP) systems.

Apart from technology, it is also important to ensure having basic controls in place, especially those highlighted in the internal audit (IA) reviews, if one has to prevent fraud. For instance, lack of control in access logs reported in IA review, if not corrected, could result in several challenges.

4 43% of all frauds are detected by tip - ACFE 2012 Global Fraud Survey

Mode of detection of fraud
(Ranks are based on total score. Rank '1' indicates most effective way)

Source – KPMG India Fraud Survey 2012

Global surveys by organisations like the ACFE have highlighted that presence of formal management reviews, employee support programmes and hotlines is inversely related to the extent of financial losses suffered due to fraud. Organisations lacking these controls experienced a significantly higher level of fraud loss.

Our survey findings highlighted that external audits of financial statements — the most commonly implemented control among the victim organisations — showed the least impact on mitigating fraud risk.

When one looks at the relationship between the presence of a preventive control and the duration of the fraud, the perpetrator's 'perception of detection' plays a vital role. The duration of frauds is considerably reduced when the perpetrators perceive that robust detection mechanisms are in place. Specifically, organisations that utilise job rotation and mandatory vacation policies, rewards for whistle-blowers and surprise audits detect their frauds more than twice as quickly as organisations lacking such controls[5]. As a result, the incidence of fraud among such companies is low as fraudsters feel the likelihood of them being caught is high.

5 2012 ACFE Global Fraud Study, 'Report to the Nations on Occupational Fraud and Abuse'

Washing dirty linen in private

One of the ways to keep fraudsters at bay is to have a robust investigation and fraud recovery mechanism. Most of corporate India tends to carry out its investigations internally, as indicated by 85 percent of our survey respondents. In our experience, an internal investigation has several challenges.

- Possible bias of the investigator as the suspect may be a known person
- Possibility of retaliation
- Availability of trained resources
- Lack of technological and other expertise to effectively gather evidence
- Lack of knowledge to handle sensitive issues

Actions taken upon detection of frauds (Multiple choices)

	Fraud Survey	
	2012	2010
The fraud was investigated internally	●	●
Implemented new or changed existing controls	◔	◑
Wrongdoers were disciplined / action taken against the vendor	◔	◔
Internal communication on the unearthed fraud and corrective action	◑	◕
Legal action taken against the fraudster	◕	◕
An external agency was hired to investigate the fraud	◕	◕
Voluntary disclosure and reporting to the concerned regulatory authority	◕	○
No action taken	○	○

● indicates >=80%; ◔ indicates >=60% and <80%; ◑ indicates >=40% and <60%;
◕ indicates >=20% and <40%; ○ indicates < 20%

Source – KPMG India Fraud Survey 2012

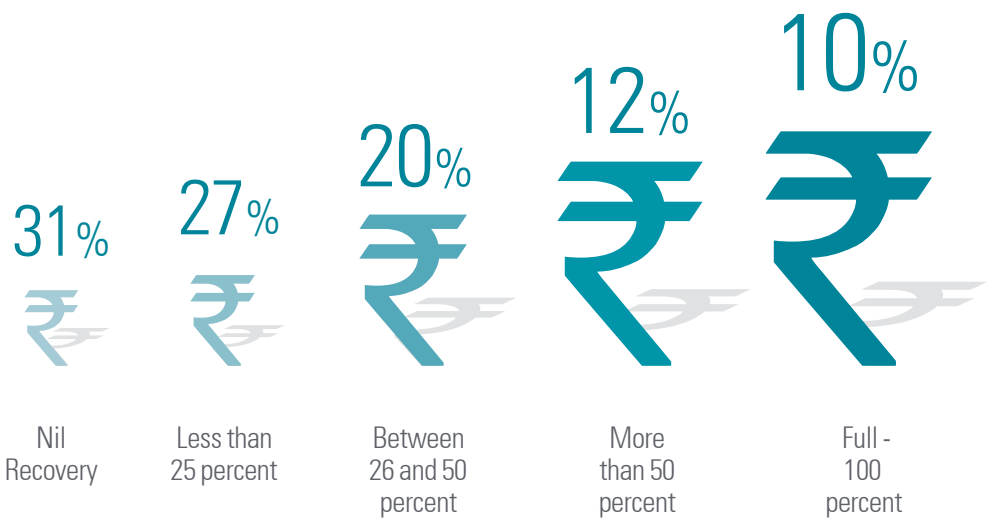
There is also little or no legal action taken in most internally investigated cases, with 69 percent of respondents opting for disciplinary action. This is because organisations are in a hurry to dismiss the fraudsters as quickly as they can to contain losses. Also, the inherent complexities (and delays) in our judicial system make it costly to pursue legal action, notwithstanding the potential loss of reputation.

For instance, Section 405 of the Indian Penal Code, which deals with criminal breach of trust, makes it mandatory to prove that the accused had a dishonest intent to misappropriate and the action resulted in a loss for the organisation. It becomes difficult for investigators to focus on adequate and admissible evidence to demonstrate the fraud beyond reasonable doubt.

Further, quantifying losses becomes a challenge partially due to the sophistication of frauds and non-availability of adequate information and/or resources. Many a times, organisations are not confident about how close their estimate is to the actual loss. For instance, as part of the procurement function how does one decide when the company has started paying higher price for an item? Which invoices were at a higher price and who were the favoured vendors? What if the price of the item was driven by the underlying commodity prices like oil price or steel price which are volatile? Not surprisingly, over a quarter of survey respondents said they were unable to quantify the extent of monetary losses suffered due to fraud.

Challenges in quantifying losses, along with little legal re-course, may result in limited recovery of the amount lost due to fraud. Of all the respondents who investigated frauds internally, 58 percent recovered less than a quarter of the estimated losses due to fraud.

Amount recovered from the fraud loss



Source – KPMG India Fraud Survey 2012

CONCLUSION

Miles to go before Corporate India sees fraud as a strategic risk

A closer review of the responses clearly indicates that although there is an increased awareness about fraud, corporate India is still hesitant to accept it as a strategic risk. It continues to be viewed as an operational risk and hence the mitigation strategies tend to be more generic rather specialist. This could be one of the key reasons for under-investment in creation of an ecosystem promoting a culture of ethics and integrity. Further, increased performance pressure both on employees as well as organisations in the current economic environment and rising aspirations have a leading role to play in the increased occurrence of fraud in most organisations. The pressure to perform in the current economic environment has never been higher and it is a fact that one needs to work much harder to get the same results.

The survey responses point out that today organisations are faced not only with the risk of traditional frauds but also substantial risks from emerging frauds. Organisations need to adopt more robust fraud risk management measures in order to mitigate the rising risk of emerging frauds. A strong technology enabled platform to provide early warning signs; adoption of ethical code of conduct amongst employees and all stakeholders; technology driven controls and a robust whistleblower mechanism are some of the ways in which organisations can mitigate the risk of fraud.

While we are seeing more and more organisations showing willingness to adopt comprehensive fraud prevention strategies, these attempts continue to be half-hearted on account of under-investment from respective organisations. In this regard, the proposed Companies Bill 2011 is a key legislation. If enacted, it is likely to prompt companies to think about having a fraud risk management policy in place. The Bill places onus on independent directors to ascertain and ensure that the company has an adequate and functional vigil mechanism. This in turn may result in companies considering controls around accounting procedures and mechanisms to prevent and detect fraud, including undertaking a formal fraud risk assessment. The most significant aspect of the Bill is the proposed stringent penalties for those perpetrating fraudulent activities. While the enactment of the Bill may happen in due course, it would be important for companies to start earlier and not wait for the regulatory push. Fraud prevention is to be treated like a journey and not a destination.

Section

02

Brushing bribery and corruption under the carpet

Why companies should be concerned

It is well known that bribery and corruption has been a concern for the Indian economy for many decades. Although, the last few years have seen publicised efforts by some corporates and the Government to create awareness about the ill effects of this malaise and discourage it, the industry by and large remains reluctant to discuss this issue. Our survey reiterates this, as about 34 percent of respondents did not share perspectives on bribery and corruption. Of the remaining, 54 percent indicated that bribery and corruption did not pose a significant risk to their organisation. Our experience says otherwise.

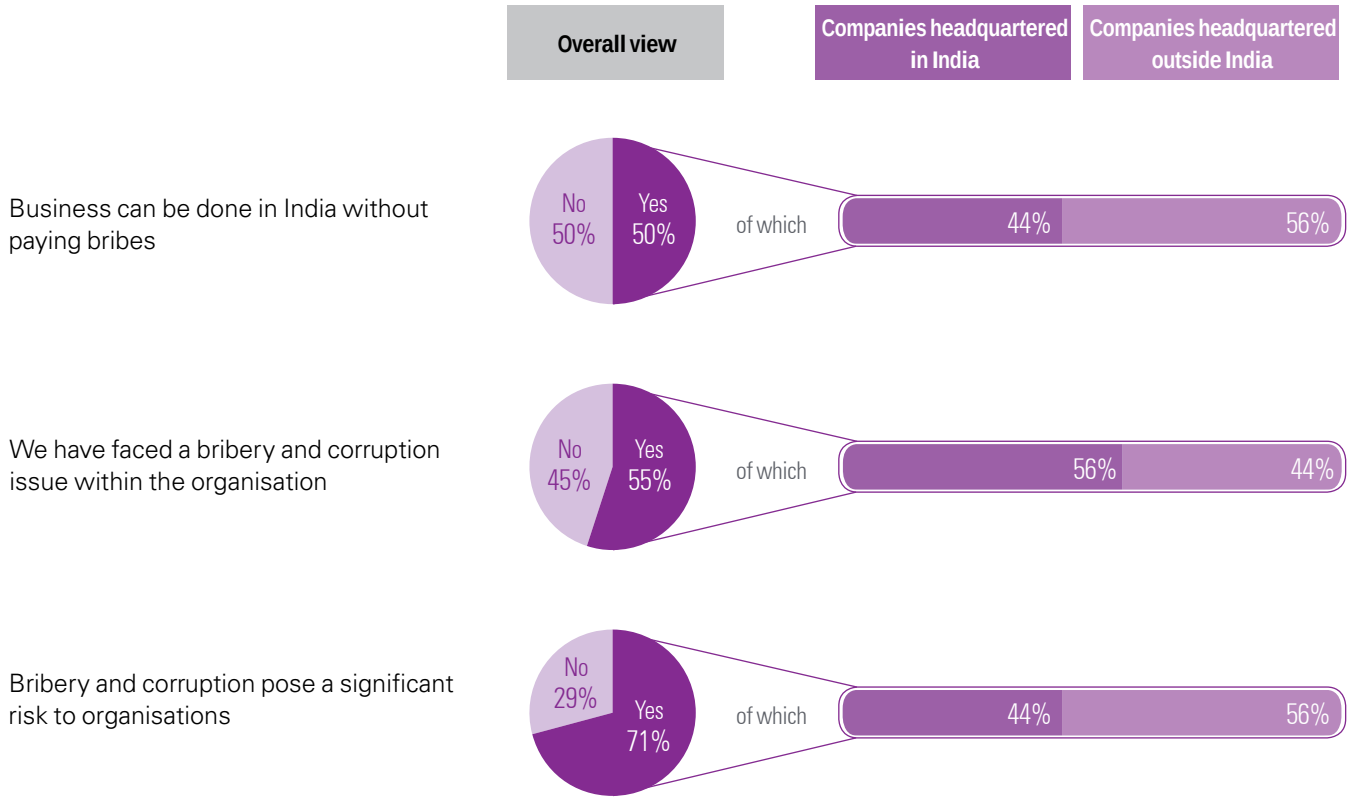
Bribery and corruption poses a very real and significant risk to companies. Tolerance to bribery and corruption reflects poorly on the company's business practices, efficiency and overall maturity in the industry as it questions the company's capabilities to operate in a level playing field alongside competition.

In the previous edition of our fraud survey in 2010, one-third of respondents stated that organisations paid bribes to win and retain business. Additionally, respondents to our 2011 Survey on Bribery and Corruption unanimously agreed that corruption skewed the level playing field and attracted organisations with lesser capabilities to execute projects, thereby endangering the health of such projects. Respondents also felt that bribery could negatively impact the performance of stock markets by increasing volatility and prevent institutional investors from making long term investments.

Globally, corruption is considered an unfair means to win over competition and reflects unethical business practices and low levels of business innovation. Countries such as the US and the UK have stringent enforcement of regulations (US Foreign Corrupt Practices Act (FCPA) and UK Bribery Act respectively) to deter companies from indulging in bribery and corruption. Some of these legislations extend their jurisdictions to entities in other countries that do business with their home-grown firms. Hence, penalties for non-compliance can include large payouts, ban on operating business in home countries, and reputational loss that impacts future business prospects.

To operate in such a milieu, multinational companies have developed basic controls and a continuous monitoring mechanism to check bribery and corruption across all their operating geographies. Such firms have demonstrated that it is possible to do business without paying bribes. Close to 56 percent of our survey respondents representing multinational firms support this view. In contrast only 44 percent of respondents representing Indian firms subscribed to this view. The chart below represents other differing views on bribery and corruption provided by respondents.

Differing views on bribery and corruption



Source – KPMG India Fraud Survey 2012

Some of these views could stem from the fact that certain industries are more tolerant of bribery and corruption than others.

KPMG VIEW

Manifestations of bribery and corruption

How does one identify a bribe? While the basic risk of a potential bribe payment exists in every company, there are variations in how this payment gets accounted for/ is justified in the books.

Our experience indicates that possible bribes are mainly payments made (through third parties and in some instances employees) to or intended to be made to public officials. Various modes of payment are adopted based on specific business and risk scenarios. An indicative analysis of manifestations of bribery and corruption, and associated challenges in detecting them is given below.

Manifestations of bribery and corruption	Monetary payment through 3rd party	Monetary payment through employee	Non monetary influence
Nature of instances	• Consultant payments • High commission payments • Inflated procurement/ service cost	• Appointing ex-Government employee as liaison officer • Inconsistent perquisites for senior management personnel	• Appointing relatives of Government employees • Unauthorised support during elections/ public events of the public official
How they are accounted	• Consultancy/ Services / Commission charges	• General Expenses • Employee Compensation	• Not Applicable
Why they don't get detected	• Absence of need assessment conducted for all service contracts • Lack of due diligence and monitoring mechanism • Lack of anti corruption clauses in commercial contracts	• Limited monitoring mechanism and periodic reviews on trends/ inconsistencies	• No known mechanism to monitor employee behavior

A recent investigation conducted by us in 2012 helped identify loop holes that can be used by employees to defraud organisations. Our client received a whistleblower complaint alleging that the Director of Procurement had received kickbacks from a particular vendor associated with a governmental enterprise. The review of documents, emails, files etc. revealed no inconsistencies whatsoever. Further an asset and lifestyle check too did not reveal any discrepancies. Finally, through market intelligence, we identified that the car being used by the wife of Director of Procurement was registered in the name of the vendor's son. Such instances can significantly dent the reputation of organisations.

External factors threaten to derail mitigation efforts by companies

Mitigating corruption is a collective effort by industry and governments and countries across the world are adopting similar mechanisms. One such aspect involves stricter enforcement of anti-bribery and corruption laws by regulators through increased prosecution. Over the last two years various regulators (DOJ or SEC of US and SFO of UK) have increased prosecution by extending the scope of their anti-bribery and corruption laws to cover corporates that fail to establish sufficient internal controls to prevent instances of bribery and corruption.

Lack of such enforcement measures can dilute the impact of anti-bribery and corruption compliance programmes and our survey respondents felt this was true in case of India. Respondents felt they were challenged in their efforts to mitigate bribery and corruption due to external factors such as 'weak law enforcement' in the country and 'lack of effective regulatory and compliance mechanisms'.

Top Five Factors Facilitating Bribery and Corruption
(Ranks are based on the total score. Rank '1' indicates most facilitating factor)

Weak law enforcement	1
Lack of effective regulatory and compliance mechanism	2
Considered as acceptable behaviour	3
Inherent nature of the industry in which the organisation operates	4
Poor internal policies, procedures and administration	5

Source – KPMG India Fraud Survey 2012

While these challenges exist, recent efforts by the Government of India including attempts to introduce specific regulation, focussed efforts to swiftly clear court cases on corruption fast, and enhancing the responsibility of Lokayuktas, demonstrate the intent to address this issue. Other supporting legislations pending with the parliament include the Prevention of Corruption Act (amendment) Bill (2008), the Whistleblower Protection Bill (2010) and Prevention of Bribery of Foreign Public Officials Bill (2011). These proposed Bills are key to bringing India on par with countries like the UK and US that have already enforced acts to prevent corruption related crimes.

While regulations can help corporate India overcome certain risks, it is also essential that organisations proactively attempt to counter corruption.

To tackle bribery and corruption organisations need to identify it as a key business concern and set up specific mechanisms to address risks from bribery and corruption. Around 72 percent of survey respondents said their organisation had a mechanism to address bribery and corruption, however, only few respondents chose to answer questions pertaining to such a mechanism. This could mean two things - that respondents were unaware of the mechanism as they had no experience of using it; or that their organisation, did not have an operational mechanism. Either way this is an indicator of moderate organisational tolerance to bribery and corruption.

Among those who elaborated on their anti-bribery and corruption framework, most respondents said that their organisations had a code of conduct specifying guidelines on payments and accepting gifts. Few had a holistic programme that included third-party reviews, due-diligence reviews and global compliance monitoring, among other aspects. The chart below details the prevention and detection mechanisms adopted by companies.

Prevention and detection framework for Bribery and Corruption	Degree of Implementation
Mechanism to report instances of bribery and corruption	◔
Anti-corruption Compliance Programme	◑
US Foreign Corrupt Practices Act / UK Bribery Act Compliance Programme	◔
Code of conduct containing guidelines on payment/acceptence of gifts and hospitality	◔
Third party due diligence / reviews on anti-bribery corruption compliance	◔

● indicates >=80%; ◔ indicates >=60% and <80%; ◑ indicates >=40% and <60%;
◔ indicates >=20% and <40%; ○ indicates < 20%

Source – KPMG India Fraud Survey 2012

Going beyond the paperwork of compliance

In the wake of anti-corruption regulations across the globe, one should realise that the risk of corruption extends beyond one's organisation to third parties such as business partners, vendors, suppliers and others. Additionally, increased stakeholder scrutiny is affecting the way companies view corruption. Stakeholders now expect organisations to go beyond the 'paperwork' of compliance (such as establishing a code of conduct and introducing periodic awareness/training sessions) to ensure effectiveness of anti-bribery measures. An example is strict adherence to the code of conduct with no exceptions.

Clearly, existing measures adopted by corporates are insufficient to comprehensively address the risks of bribery and corruption and organisations need to do more. Some measures that organisations can include in their compliance programmes are as follows:

- Drawing up a comprehensive code of conduct communicating the organisation's zero tolerance attitude to corruption
- Imbibing the "Integrity Pact" (a Transparency International initiative) to fight corruption in private contracting and procurement and agreement to participate in Extractive Industries Transparency Initiative (EITI) (if applicable).
- A structured whistle blowing mechanism to report potential bribery / corruption issues
- A comprehensive and periodic risk assessment mechanism alongside a concurrent monitoring mechanism, including third party audits with specific reference to corruption related risks
- Develop and train employees and third parties periodically on the compliance requirements and consequences of non compliance

Section

03

Emerging Fraud Risks – the ugly truth

Cyber crime is the big daddy of all emerging frauds

Over the last decade knowledge has emerged as a key organisational asset and it is increasingly being targeted by fraudsters. Our survey respondents rated cyber crime (53 percent), Intellectual Property fraud, including Counterfeiting and Piracy (38 percent) and Identity theft (34 percent) as the top fraud concerns for the future. We believe this is due to the proliferation of knowledge as a key organisational asset. All three frauds identified by respondents target such organisational knowledge. Companies must hence identify their sensitive information assets, classify them appropriately based on vulnerability and put in place the necessary protection measures to prevent such frauds.

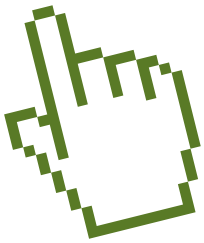
Top emerging fraud risks

1 Cyber crime

2 IP, Counterfeiting and piracy

3 Identity theft

Cyber crime



Cyber crime comprises any form of crime where either the tool or the target of the crime is a computer or a computer network.

Cyber crime is fast becoming a popular way of defrauding both individuals and entities. No business or individual with an online presence can be considered as completely secure. Perpetrators typically either attempt to steal money, or more seriously sensitive data from target companies. In some instances, cyber attacks are also aimed at disrupting vital operations and critical functions in target organisations, leading to not just financial loss, but also loss of customer confidence and market reputation.

At the lower end of the spectrum, many of us have received emails that appear to have been sent by our respective banks or from the banking sector regulator or the tax authorities. These emails often contain urgent requests to validate or share our internet banking usernames and passwords. In some instances, these emails may contain instructions to transfer some money to a certain account. One is threatened with closure of bank accounts or other legal action in case of non-compliance with the instructions mentioned. This type of communication is classified as 'Phishing' and is a common type of cyber crime.

Over 70 percent of our survey respondents indicated they had heard or experienced cyber crime of this nature. Of late, fraudsters have also started targeting cell phones and handheld devices through SMSs (called Smishing[6]) and voicemails (called Vishing[7]). According to statistics from the National Crime Records Bureau, cyber crime cases in India have increased eight-fold between 2007 and 2011, prompting authorities like the RBI to issue advisory to customers cautioning them against such incidents.

In more serious instances, such emails carry malware that allows the attacker to gain access to and compromise not just the computer, but at times, the company's network as a whole.

6 Phishing through SMS

7 Phishing through voice mails

Intellectual property fraud, counterfeiting and piracy

We are a knowledge economy where intangible assets (intellectual property, R&D capital, brand equity, etc) constitute a significant proportion of a firm's total assets. A study by The Conference Board[8], a public interest business research and insights firm, of 633 US-based research and development intensive companies revealed that book value now comprises only a small proportion of a company's market value[9]. Specifically, intellectual property such as inventions, trademarks, industrial designs, geographic indications of source and copyrighted material can comprise a significant portion of intangible assets and therefore market value. The study quotes the example of the pharmaceutical sector where for some companies as much as two-thirds of their market value comprised of intangible assets.

This being the case, any theft or counterfeit of intellectual property could adversely affect companies. A recent World Customs Organisation[10] report[11] highlighted that, globally, in 2011 over 25,500 cases were reported involving the seizure of more than 143 million counterfeit and/or pirated articles. The study further indicated an increase in counterfeits of pharmaceutical products, and mobile phones and their accessories. In India counterfeits could comprise as much as 50 percent of all products one uses. It is therefore not surprising to note that 38 percent of our survey respondents have highlighted intellectual property fraud, counterfeiting and piracy as areas of concern in the future.

Identity theft

Identity theft is committed by accessing personally identifiable information of individuals/ entities without their permission with the objective to misuse this information and gain undeserving benefits.

One of the primary reasons for growth in identity theft has been the proliferation of the Internet. In India, the number of internet users has grown from 7 million in 2001 to over 98 million by 2011[12] and is expected to reach the 300 million mark by 2015[13]. However, controls and regulation aimed at protecting privacy have not kept pace with this growth. Fraudsters are making use of these gaps in controls to target individuals and organisations and misuse confidential data. According to the Norton Cybercrime Report 2011, four out of five online adults in India were victims of identity theft in 2011[14]. Considering that many employees in the corporate work force use their office laptop/ computer for personal transactions (such as online banking, shopping, payment of bills etc), identity theft can compromise not just their private information, but also the companies they work for.

8 Intangible Capital and the 'Market to Book Value' puzzle, Charles Hulton and Janet Hao, The Conference Board, June 2008

9 'Issues in Intangibles – Measuring What Counts', The Conference Board, Winter 2012

10 The World Customs Organisation (WCO) is an intergovernmental organisation representing collective thinking of customs organisation of several countries

11 'WCO Customs and IPR Report 2011', The World Customs Organisation, July 2012

12 Economic Intelligence Unit database

13 'Indian internet industry sees 300m users by 2015', The Times of India, 31 December 2011

14 'Cyber crime: Beware of ID theft', The Economic Times, 27 January, 2012

Majority of the sectors rate cyber crime as top risk

A sector-wise heat map of emerging frauds reveals that nearly two-thirds of the industry segments rated cyber crime as the top most concern for their organisation, while nearly half of them rated IP fraud, counterfeiting and piracy as the second most important concern. Not surprisingly, respondents from consumer markets and telecom industries rated IP fraud, counterfeiting and piracy higher than other industry-respondents.

Sector Heat Map of Emerging Frauds

Industries	Cyber Crime	IP fraud, counterfeiting and piracy	Identity theft
Consumer markets			
Financial services			
Healthcare			
Industrial markets			
Information and entertainment			
Real Estate & infrastructure			
Social sector			
Telecom			
Travel, tourism and leisure			

High Risk **Low Risk**

Source – KPMG India Fraud Survey 2012

Overall real estate and infrastructure, financial services, and defence emerged as sectors that respondents felt were most prone to cyber crime. This could be due to the perception of these industries being susceptible to fraud at large, including well known frauds such as procurement, siphoning of funds etc.

Taking the fight to the finish – Combating fraud

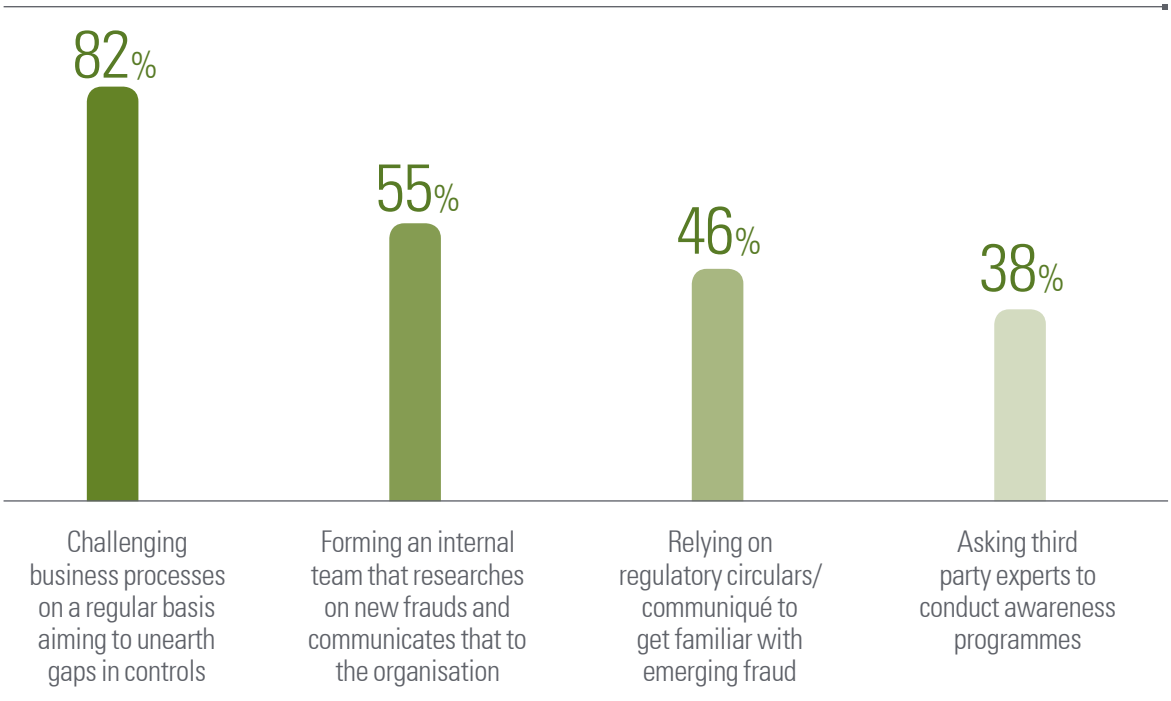
Two approaches better than one

Most organisations are relying on internal initiatives to keep themselves abreast of emerging fraud trends. While 82 percent of the respondent organisations are challenging business processes to unearth gaps in existing controls, another 55 percent are forming an internal team to research on emerging frauds and communicating them within the organisation.

There is high reliance on internal mechanisms to detect and prevent emerging frauds. This is evident from the fact that steps such as whistle-blower mechanism and a framework to monitor compliance of company's code of conduct have been either fully or partially implemented by the respondents in our survey.

A limited number of respondent organisations are relying on external initiatives such as regulatory circulars or hiring third-party experts to conduct awareness programmes. In our experience, internal teams are limited in their skill-sets and experience. Hence, to have a more robust preventive framework, an optimal mix of internal and external initiatives would be beneficial.

Measures taken to familiarise with emerging frauds (multiple choice)



Source – KPMG India Fraud Survey 2012

One-size-fits-all risk management frameworks fail to address emerging frauds

A preventive framework cannot be developed through a one-size-fits-all approach. It would differ based on the size of the organisation and the sector in which it operates. A majority of companies, irrespective of size and sector, tend to rely on general process controls and compliance frameworks as a method of combating even emerging frauds. To create a robust framework one needs to look beyond these measures, such as comprehensive information security measures, protection of personal information, physical security measures, and robust access protocols, along with periodic reviews. Large organisations, specifically those in the financial services sector would be better off with a dedicated fraud control unit that uses data analytics extensively to create an effective preventive mechanism. Companies in the IT/ITES sector can rely on the process of employee/third-party due diligence.

Analysis of survey responses by sorting them based on the industries represented suggests that the financial services industry appears to be ahead of the pack, with more than half of the respondents indicating that they have established a dedicated fraud investigation unit and a process for conducting employee/third-party due diligence. This sector deals with extensive transactional volumes which requires more focussed technology based assessments that enable key red flag identification.

Emerging Fraud Risk Management Mechanism	Degree of Implementation
Introduce process-specific fraud controls	◐
Employees and third party stakeholder due diligence	◐
Implement a whistleblower mechanism/fraud reporting hotline	◐
Establish a framework to monitor and ensure compliance of the company's Code of Conduct / Code of Ethics	◐
Conduct fraud awareness trainings by third party experts	◔
Set up a dedicated/separate fraud investigation unit	◔
Forensic audit by third party	◔

● indicates >=80%;
◔ indicates >=60% and <80%;
◐ indicates >=40% and <60%;
◔ indicates >=20% and <40%;
○ indicates < 20%

Source – KPMG India Fraud Survey 2012

Data analytics is globally acknowledged as an important tool to help detect fraud and non-compliance across organisations. While respondents realise its value and are inclined to implement it, the majority said their organisations had not yet fully implemented it. Currently respondents use data analytics only for common frauds such as those around procurement. They would however, need to tailor data analytics solutions to tackle emerging frauds.

Processes where Data Analytics is Utilized	Degree of Implementation
Receivables and collections	◐
Sales and distribution	◔
Vendor and payments	◐
Payroll and re-imbursements	◐
Time and physical access controls	◐
Emails and external communications	◐

● indicates >=80%;
◔ indicates >=60% and <80%;
◐ indicates >=40% and <60%;
◔ indicates >=20% and <40%;
○ indicates < 20%

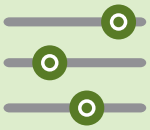
Source – KPMG India Fraud Survey 2012

KPMG View

Making technology work for you

The merits of implementing a technology based framework to prevent, detect and mitigate fraud risks have been widely acknowledged. However, most organisations hesitate to implement newer technology tools to track anomalies across their processes and data. This may be because they are unsure of the benefits of adding yet another tool to the existing labyrinth of software. Investments in any new fraud detection tool may also take a back seat due to IT expenditure being focused on business rather than controls.

Can companies do better with the software / tools they already have? Yes. In our experience companies often tend to underutilise the scope and effectiveness of their existing enterprise software. Some simple measures that organisations can take to use their existing technology better are as follows.



1. Aligning the MIS

Management Information Systems capture a wealth of data and offer various options to present this data in the form of reports. Most organisations are limited in their ability to analyse this data or present them in a manner that is more relevant to their fraud risk management strategy.

2. Leveraging the ERP system

Currently the ERP systems used in most organisations are operated by a limited set of people primarily for book-keeping purposes. However, the scope of an ERP is much more than that. In our engagements we have often seen companies rely heavily on offline data in worksheets and other documents. This makes detection of red flags complex as offline data is not integrated with other data in the organisation, requiring manual verification.

3. Comparisons with other data sources

Aside from the ERP, organisations have a lot of other tools that work on data to generate meaningful information. These differ from the data in the MIS and should be periodically cross checked to detect any gaps/ anomalies / duplicates. Gaps may indicate potential fraud.

Section

03A

Cyber Crime – robbing organisations blind

Cyber crime incidents are on the rise across the world and India is no exception to this trend. As per Norton's Cybercrime Report 2011, cyber crime cost the global economy (in both direct damage and lost productivity time) USD 388 billion in 2011. India is estimated to have damages of USD 7.6 billion (INR 341 billion) due to cyber crime in 2011. The high cost of cyber crime is a direct result of the number of people defrauded by it. Norton's Cybercrime Report mentions that close to 30 million people were affected by cyber crime in 2011 in India as against 431 million globally.

India has seen an increase in the number of cyber crime cases filed. In 2011, a total of 1,791 and 422 cyber crime cases were registered under the Information Technology Act, 2000 and the Indian Penal Code respectively, as opposed to 217 and 328 in 2007[15]. In keeping with this data, around 38 percent of our survey respondents said they had experienced cyber crime in the last one year.

15 'Crime in India', National Crime Records Bureau, June 2012

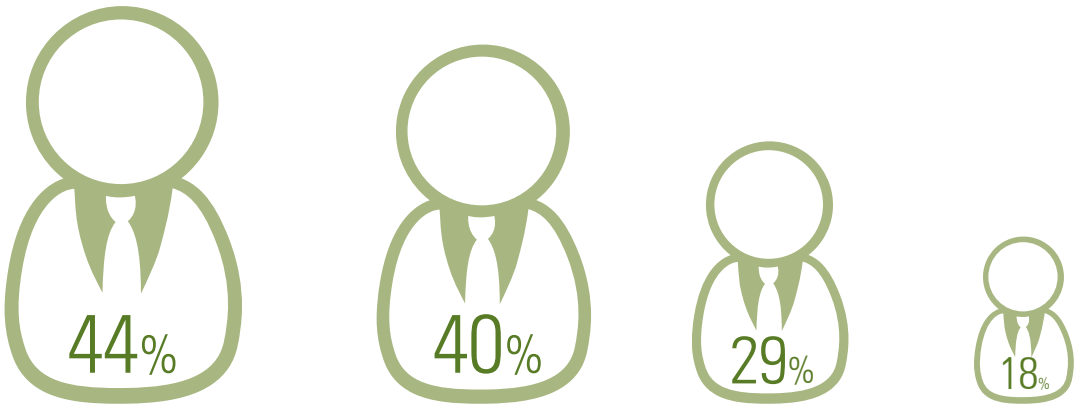
Over a third of respondents have experienced cyber crime

When asked who they felt perpetrated cyber crime, 44 percent of respondents indicated that employees were responsible for perpetrating cyber crime, while 40 percent said external parties were the perpetrators. It is interesting to note that more respondents rated the "enemy within" higher than external perpetrators.

Although our survey did not specifically delve into aspects such as the profile of cyber crime perpetrators, based on our experience it would be fair to conclude that the average perpetrator would be in the age group of 18 -30 years.

This is also reiterated in the data available with the National Crime Record Bureau, where 58.6 percent of the 1184 people arrested under the Information Technology Act, 2000 and 42.1 percent of the 446 people arrested under the Indian Penal Code in 2011 for perpetrating acts relating to cyber crime were in the age group of 18-30 years.

Who is responsible for perpetrating the majority of cyber incidents in your organisation?



Source – KPMG India Fraud Survey 2012

Customer Data theft giving firms sleepless nights

Cyber crime can manifest itself in many ways. Respondents were most familiar about data theft (80 percent), network Intrusions/hacking (76 percent) and virus/malware (76 percent) as ways cyber crime could affect their organisations, possibly because of the media coverage of such issues. These concerns appear to be in line with global trends, where hacking (81 percent) and malware (69 percent) continue to remain the most common manifestations of cyber crime.

Ways in which Cyber Crime can affect organisations (Multiple Choice)

Source – KPMG India Fraud Survey 2012

Further, respondents across sectors placed customer data at the top while listing key high-risk targets of an electronic attack. While sensitivity towards customer data is naturally high, other key information assets such as personally identifiable information, access information etc. should also be viewed as equally high-risk targets. A recent undercover investigation by a media agency highlighted the sale of sensitive personal data of overseas customers by certain call center employees. According to the report, the data on offer included confidential account details from major financial institutions, transaction details and computer IP addresses among other things . Such data could potentially be worth millions of dollars. Worse, it could bring businesses to a grinding halt, if customers came to know of such practices.

16 'Data thefts threaten all Indian call centres',MarketingWeek, 20 March 2012

Similar news items about online stores and web portals being compromised have become common. At times, organisations are not even aware that their networks have been compromised and that data or information may have been stolen.

Such instances highlight that it is not sufficient to look at just the technical aspects of cyber crime. One must also realise that human intervensions play a big role in committing cyber crime. Organisations should therefore go beyond plugging IT vulnerabilities to include a holistic policy that covers employees also. For instance, there can be policies discouraging sharing of login/password information and these should be stringently enforced. Additionally, companies should have provisions to safeguard personal information, adopt robust overall information security measures, and conduct periodic reviews of process controls to ensure any gaps are identified early on and plugged.

Cyber Crime Risk Heat Map

Assets at Risk	Degree of Risk
Customer data	
Intellectual property	
Company information e.g. Legal / Financial information	
Business sensitive information e.g. Profit and Loss figures	
Personal identifiable information of employees	
Login/password information	

High Risk **Low Risk**

Source – KPMG India Fraud Survey 2012

Top five IT vulnerabilities

1. Connection to and from the internet
2. Applications hosted on the web
3. E-mail records
4. Mobile data devices
5. Maintainance acess to systems from contractors/ third parties

Source – KPMG India Fraud Survey 2012

Hunting an elephant with a water pistol

A study conducted by Ponemon Institute in partnership with Symantec revealed that Indian organisations spent an average of INR 53.5 million to remediate a data breach . This shows how costly a reactive approach to cyber crime can be. However, preventing cyber crime is difficult due to the technological complexities involved and the fact that a large population needs to be controlled including customers or other connected service providers, who may be careless or ignorant about the effects.

Further, preventing, tackling and mitigating cyber crime incidents are seen as the responsibility of the information security team, as indicated by 91 percent of respondents. This is challenging as the information made available to such teams (for investigation or establishing preventive mechanisms) is often internal company data and not the vulnerabilities or information access patterns of customers or business partners (classified as third party data). Therefore utilising limited data for investigating breaches does not help get an accurate picture of the gaps in the control systems. Also specific skills are required to investigate cyber incidents. In our experience, however, most internal information security teams use IT administrators and network security professionals to investigate cyber attacks – something they are not trained to handle.

An IT incident response policy primarily focuses on identifying the root cause of an incident and restoring operational capability at the earliest. However, cyber crime related incidents have to be dealt in a manner which involves forensic technology methods with emphasis on evidence preservation and quarantine procedures. Organisations would have to take a different approach to this including using different skill sets, tools, and procedures.

Prevention and Detection Framework for Cyber Crime	Degree of Implementation
Ability to trace access logs for various critical systems	◔
Control over access to personal email accounts/external Websites	●
Ability to log all external websites accessed by employees from the company's network	◔
Control of spam/malicious emails through appropriate filters	●
Utilisation of advanced encryption on office laptops	◔
Existence of periodic review of IT security policies	●
Existence of cyber incidence response policy	◐

● indicates >=80%; ◔ indicates >=60% and <80%; ◐ indicates >=40% and <60%;
◔ indicates >=20% and <40%; ○ indicates < 20%

Source – KPMG India Fraud Survey 2012

Awareness will help companies equip themselves better

Organisations can create awareness about cyber crime by setting the tone at the top. Boards have a fiduciary duty of safeguarding not only the physical assets of the company, but also information assets. If Boards have an obligation to ensure that the corporate office/plant is secured, they also have an obligation to ensure that the digital door is locked.

In late 2011, the SEC issued guidelines that require public companies to disclose security events if they materially affect the entity's products, services, relationships, or competitive conditions or if they would make an investment in the company that is viewed as risky because of some of these reasons.

In line with this, Boards were asked to ensure that information risk management was integrated into an entity's enterprise risk management strategy.

Across the globe, governments too are prioritising cyber security as both a national security and economic security issue. The US federal government is ramping up its cyber security workforce and forecasts spending USD13.3 billion on cyber security initiatives by 2015[18]. India too has initiated action in this regard with the proposed policy for national cyber infrastructure protection. The policy envisages establishment of sectoral Computer Emergency Response Team (CERT) to respond quickly to protect critical assets such as power distribution networks, air traffic controls, traffic networks, etc. It also envisages creation of the National Critical Information Infrastructure Protection Centre (NCIPC) for ensuring protection of critical information and communication assets.[19] This could spur companies to look at creating similar programme at a company level for their data protection.

At an organisational level, companies can start by setting a clear policy on information assets, including what they are, how an employee must use them, who do they belong to and what happens in case those assets are lost or compromised. Another aspect is conducting regular training programmes. Workshops as well as e-learning modules can be made available to employees to help them identify potential cyber crime related risks/ scenarios. Trainings can also be conducted by experts to drive home the importance of preventing cyber crime.

It is in the interest of companies to have an incident response plan, which defines a clear set of steps to be taken by the organisation in the event of a security breach.

Lastly, organisations must set up a separate specialist team with prior experience of handling cyber breaches, to handle their cyber security and conduct investigations into any breaches. Alternatively, they can also hire specialist agencies to do this for them.

18 '2012: Year of war against cyber crime', The Economic Times, 16 February 2012
19 'India to add muscle to its cyber arsenal', The Times of India, 11 June 2012

Section

03B

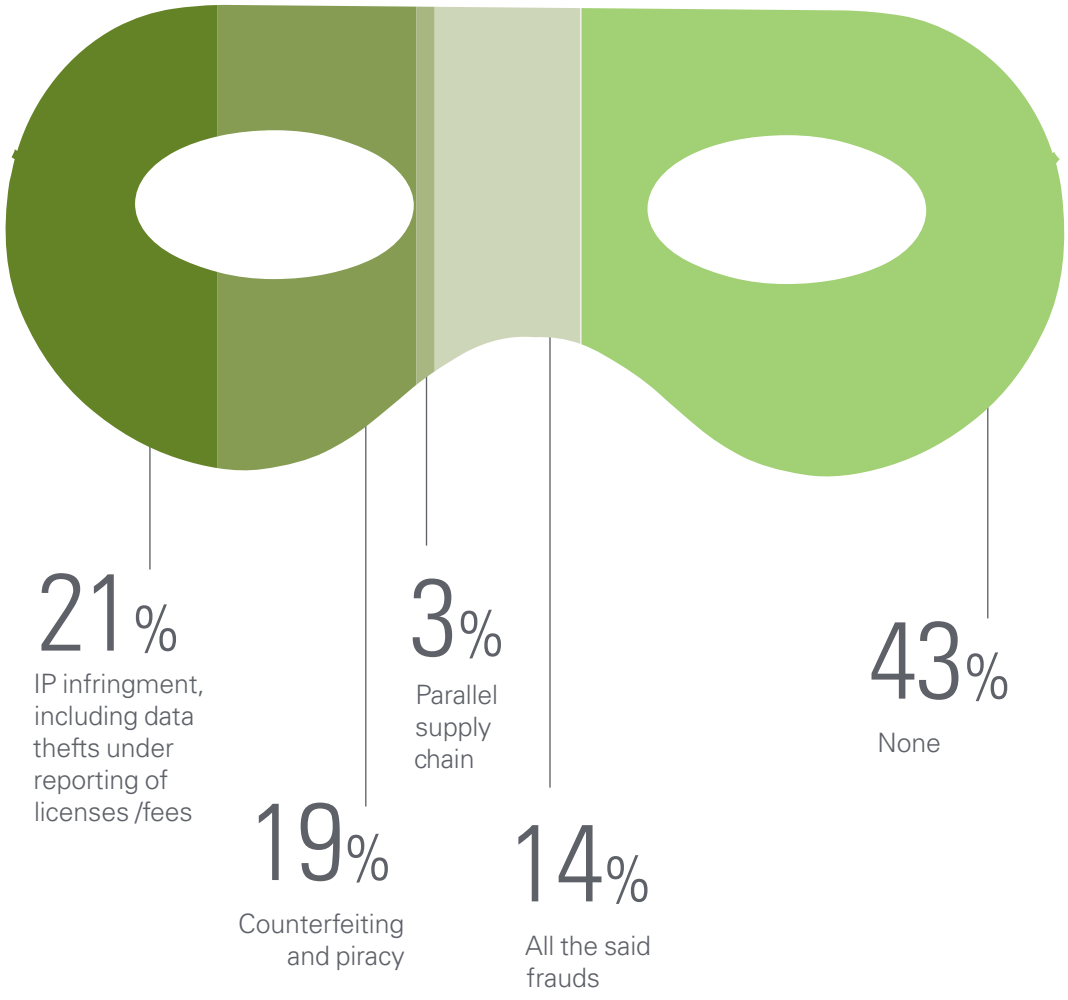
IP Fraud, Counterfeiting and Piracy – the white elephant in the room

Intellectual property fraud, counterfeiting and piracy are rampant in India. Counterfeit and pirated goods in India are estimated to be worth over USD 5 billion,[20] according to the Havoscope Global Market Index. Various reports suggest that this type of fraud is only increasing, thanks to the enormous profits it offers in return for a small upfront investment and little other business risks. Additionally, the low penalty and prosecution levels in India for IP fraud provide little or no deterrence against further infringements[21]. While companies seem to be aware of piracy and counterfeiting, there is little understanding of how such practices can impact their business.

20 'Fighting the crime of the 21st century', World Trademark Review, April/May 2012
21 'Special 301 Report', Office of the United States Trade Representative, 2012

It is therefore not surprising to find that nearly 78 percent of survey respondents were unaware of the risks of IP infringement/counterfeiting/piracy. Among those who were aware, a majority of respondents (57 percent) indicated that they had experienced IP infringement or counterfeiting/piracy in the last one year. Of these, two-thirds indicated that they had faced between 1 to 10 such fraud incidents, underscoring that this type of fraud is quite widespread.

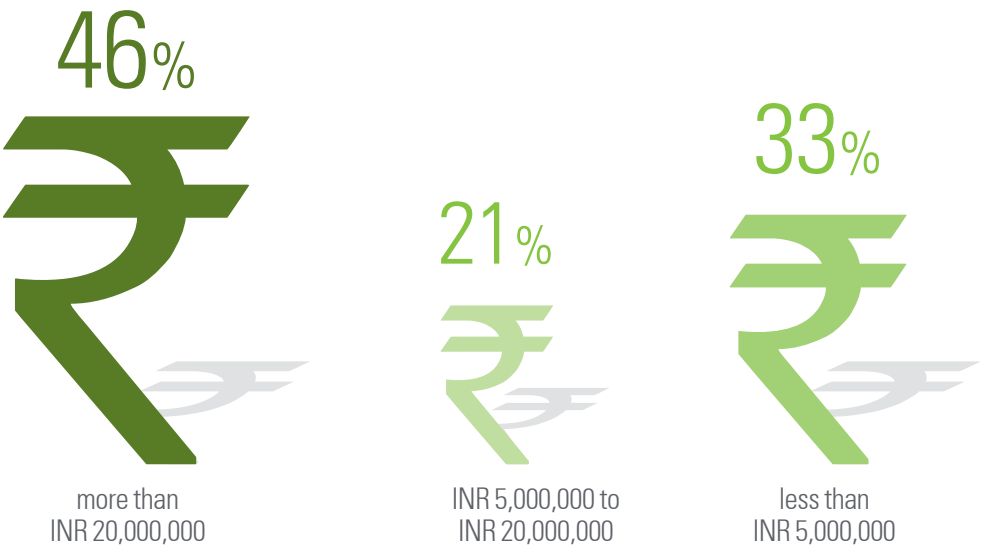
Frauds experienced in the last 12 months?



Source – KPMG India Fraud Survey 2012

Of the respondents who were aware of such risks, around 77 percent said that such a fraud could adversely affect the brand/reputation of their organisation. Around 46 percent of respondents estimated the direct monetary loss on account of IP fraud, counterfeiting and piracy to be a little over INR 20 million. In our experience losses are significantly higher, and respondents' choice in this case may be an indication that they are unaware of how to estimate losses from this type of fraud.

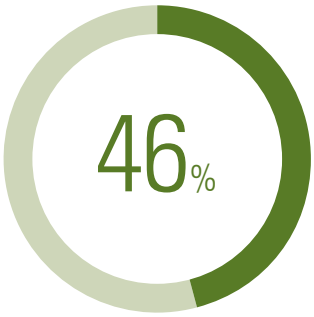
How much do you think organisations can lose directly through incidences of IP infringement, counterfeiting/piracy?



Source – KPMG India Fraud Survey 2012

Respondents considered the source of such fraudulent activities as primarily internal as they rated 'employees' over 'competition' as parties who pose maximum threat of IP fraud. This is in contrast to our 2010 survey where the respondents had rated 'competition' over 'employees' as posing the maximum threat.

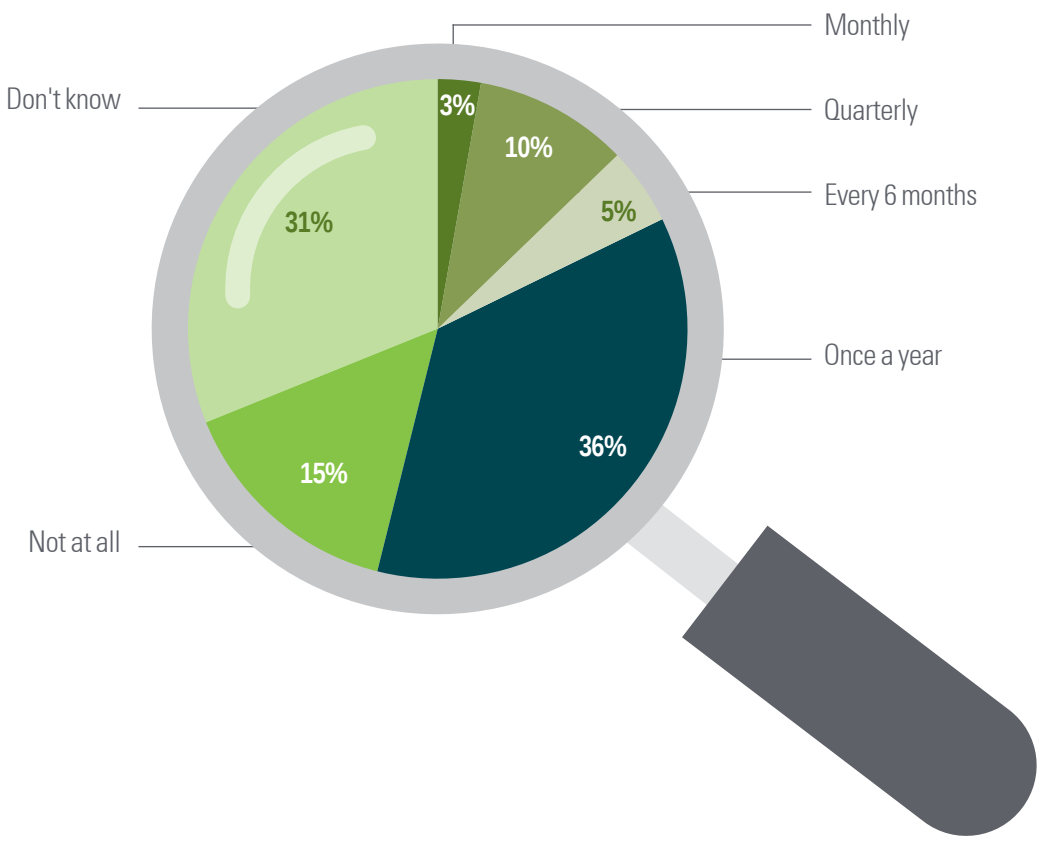
Low awareness of risk assessment and mitigation procedures



Do not perform or are not aware of annual risk assessment for IP infringement

Only a little over a third of the respondents indicated that they performed an annual risk assessment for IP infringement along with a market survey and supply chain analysis to address counterfeiting and piracy issues. Nearly half of the other respondents were either unaware of such an assessment or believed it was not performed in their organisation.

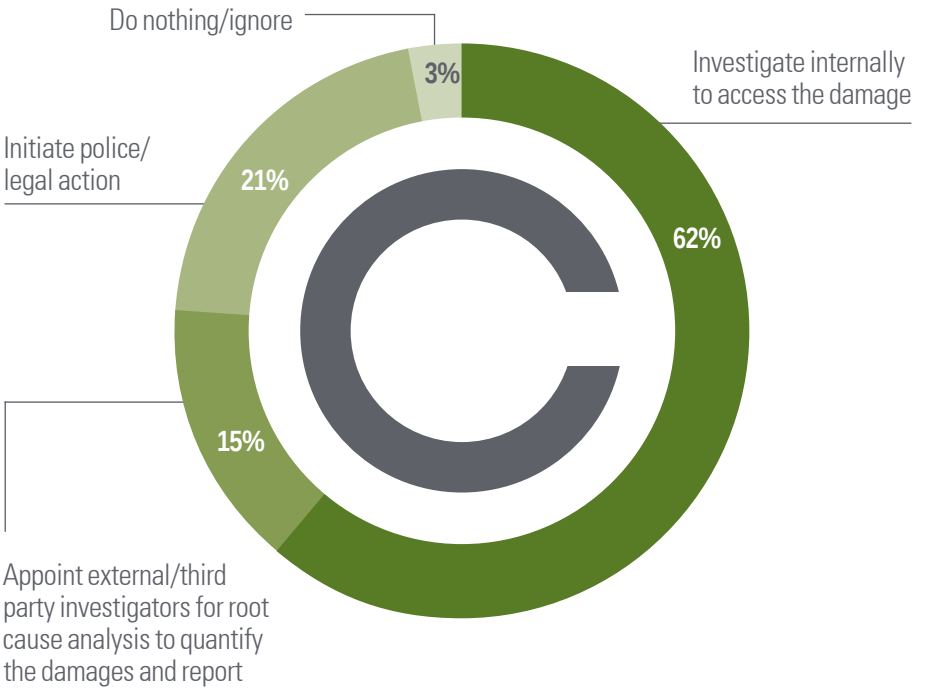
Frequency of performing a risk assessment to address counterfeiting and piracy issues



Source – KPMG India Fraud Survey 2012

Upon detection of an incidence of IP fraud/counterfeiting/ piracy, around 62 percent of respondents said they initiated an internal investigation as against 15 percent who appointed external third-party investigators. Only a limited proportion (21 percent) of respondents said they initiated police/legal action post investigation.

Actions taken upon detection of IP infringement, counterfeiting or piracy issues



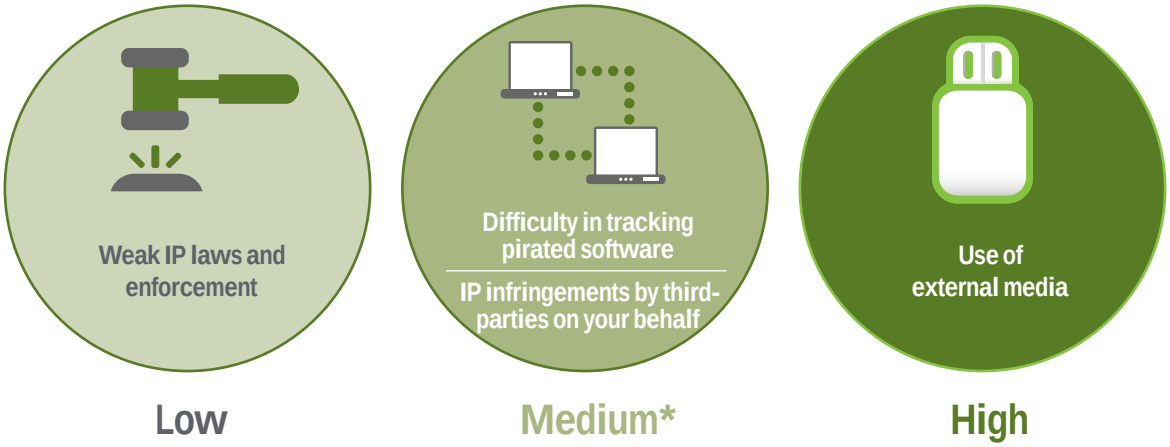
Source – KPMG India Fraud Survey 2012

While all this collectively reflects the low awareness organisations have about the impact of these risks, respondents were asked to rate the challenges they faced in protecting IP.

They rated 'utilisation of hard-to-trace external media' and 'difficulty in tracking use of pirated software' as the main challenges in protecting the IP of an organisation. IP infringement by third-parties was also rated as a challenge.

This assessment is a result of assuming/ categorising these risks as external risks that the company has little or no control over. This view is not entirely correct because there are many globally acknowledged risk management frameworks that can be implemented internally at various organisational levels to tackle IP fraud, piracy and counterfeiting.

Top three issues in protection of IP



Source – KPMG India Fraud Survey 2012

* These issues have been rated equally

Reviews, training and awareness viewed as effective counter measures

Respondents having a risk management mechanism in their organisation rated license compliance reviews and contract compliance reviews as the most effective measures to prevent and detect IP fraud. They also believed that counterfeiting could be tackled through a three-point agenda that included establishing appropriate policies and procedures, increasing awareness through training sessions for employees and distributors, and patent/trademark infringement actions. (See charts below)

Measures to prevent and detect IP fraud	Degree of effectiveness
License compliance reviews	◔
Contract compliance reviews	◔
Review of legislative compliance (Patents/Copyright etc.)	◐
Channel reviews	◔
Training of employees	◐
Awareness campaign for customers	◔
Conduct raids against counterfeit/pirated products in the marketplace	○

● indicates >=80%; ◔ indicates >=60% and <80%; ◐ indicates >=40% and <60%;
◔ indicates >=20% and <40%; ○ indicates < 20%

Source – KPMG India Fraud Survey 2012

Anti-counterfeiting initiatives/actions to undertake	Degree of effectiveness
Patent and trademark infrigement actions	
Customers, company and industry awareness programme	
Procedures and policies for detecting and reporting suspects products	
Training programme for employees, distributors and packers	
Working with industry and trade associations for brand protection	
Tracking suspected and confirmed counterfeit products	

indicates >=80%; indicates >=60% and <80%; indicates >=40% and <60%;
indicates >=20% and <40%; indicates < 20%

Source – KPMG India Fraud Survey 2012

Further, from a policy perspective, since former employees who join a competitor pose the highest risk, it may also make sense for companies to have a robust exit mechanism which includes completing a legally binding non-disclosure agreement. Some companies are known to perform surprise checks during the notice period of an existing employee which in certain cases involves a review of emails sent from his/her personal email account.

Thus, a strong enforcement framework that includes creating awareness of such frauds along with strict action (legal or otherwise) will go a long way in curtailing IP fraud, counterfeiting and piracy.

Section

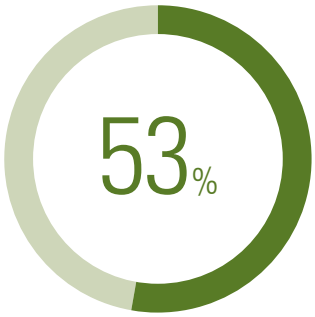
03c

Identity theft – Mitigation frameworks wet behind the ears

A 2011 survey of young professionals in India revealed that one out of four is a victim of identity theft[22]. Another recent study[23] highlights that while the amount of monetary loss due to identity theft has remained steady, the frequency of identity theft incidents has increased by 13 percent in 2011.

22 'India ranks highest in flouting IT regulations at workplace, reveals Cisco study', Information Week, 15 December 2011

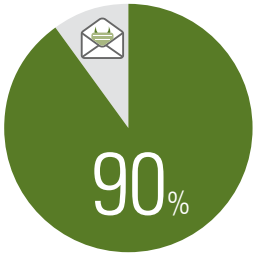
23 '2011 Identity Fraud Survey Report' Javelin Strategy and Research, February 2011



Organisations have faced identity theft

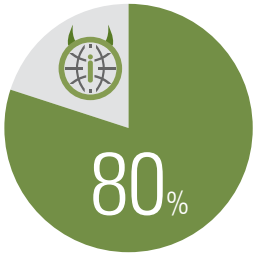
In keeping with this, over half of our survey respondents indicated that their organisations had faced identity theft in the last one year. Additionally, respondents were aware that phishing e-mails, password sharing between team members and malicious websites were some of the most common means through which identity theft is perpetrated. However, there was comparatively lower awareness of sophisticated means of identity theft such as mining personal data from discarded/ exchanged mobile phones.

What are the ways in which identity theft can occur[24]?

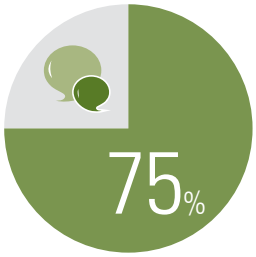


Phishing emails

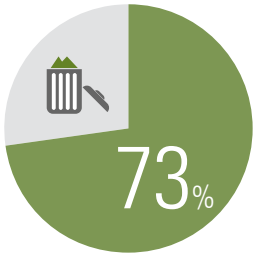
Password sharing between team members



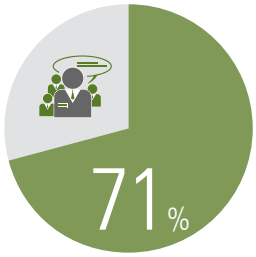
Malicious websites



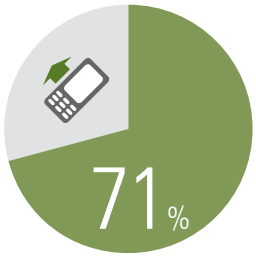
Social media sites



Documents in your waste paper bin

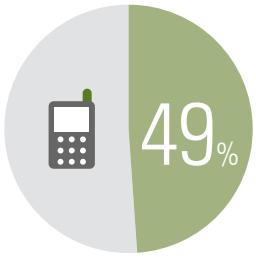


Social engineering (tricking people to break security measures



Over the phone

Malware (key loggers, worms)



The old mobile phone you exchanged for a new one

Source – KPMG India Fraud Survey 2012

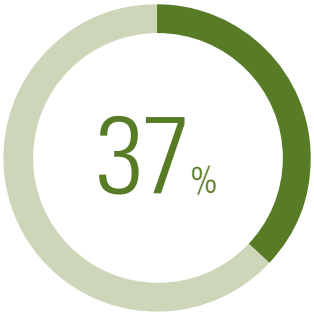
24 Social engineering could involve misrepresenting as employees of a particular company and floating fake orders or loans taken in the name of and with collateral of someone, besides other modus operandi.

A common type of identity theft that has been increasingly witnessed involves impersonating or cloning websites to defraud people. The fraudulent website is a clone of the original one, but with dubious intentions. Such clones have known to attack payment systems and online credit card processing systems to launder money and fund crimes such terrorism, drug trafficking and illegal immigration, besides peddle counterfeit goods. Recently, the Counterfeiting Intelligence Bureau of the International Chamber of Commerce launched a new service to shut down websites that cloned those of its member firms[25]. The US Internal Revenue Services (IRS) puts out advisory that helps visitors identify online scams that impersonate the IRS.[26] Many Indian government sites have also seen clones surface in the past.

Password sharing biggest culprit leading to identity theft

Of the organisations which faced identity theft, 37 percent identified password sharing as the primary cause, followed by social engineering (19 percent) and malwares (11 percent). Consistent with this view, another recent study[27] identifies social media and mobile technologies as one of the major channels for committing identity theft.

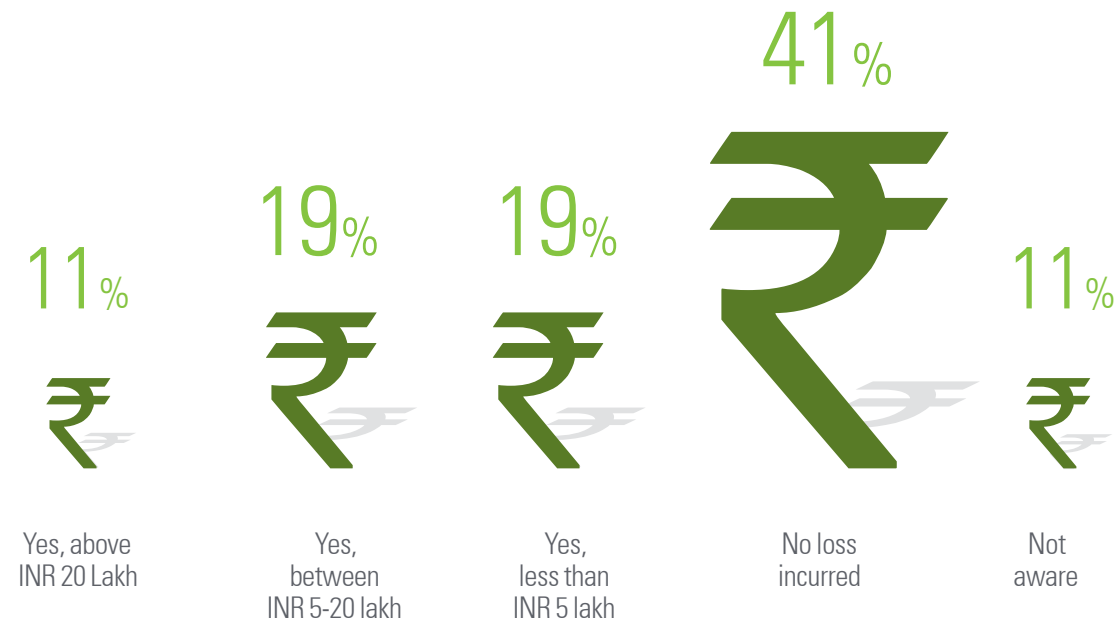
While company proxy servers, internet security applications and firewalls help in controlling external exposures due to phishing or other malicious websites to a certain extent, few organisations are aware of the kind of controls that they can implement on password sharing. The issue is further complicated by 'officially sanctioned password sharing' that occurs due to the limited number of licenses of a particular software. There are instances where maker-checker protocols are breached through such password sharing, creating additional issues for organisations.



Organisations identify password sharing as a primary cause of identity theft

25 ICC Press release , May 9, 2012 - http://www.icc-ccs.org/news/739-cib-launches-new-service-to-shut-down-clone-websites
26 IRS Update on Phishing and Malware, February 2010 - http://www.irs.gov/newsroom/article/0,,id=217794,00.html
27 '2011 Identity Fraud Survey Report', Javelin Strategy and Research, February 2011

Did you face a financial loss due to the incident?



Source – KPMG India Fraud Survey 2012

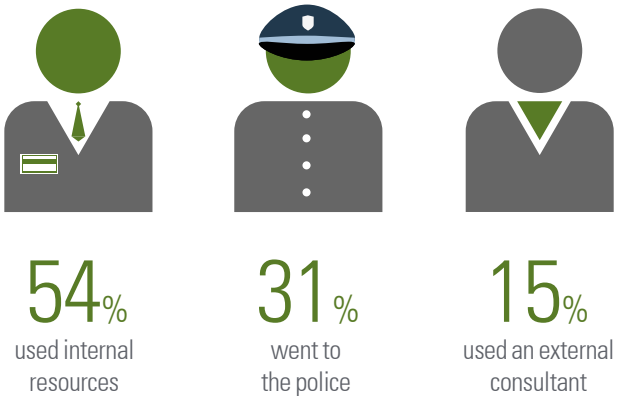
In case of an incident where the Internet is utilised to commit identity theft, it may be easier to identify the perpetrator due to the electronic trail left by him/her, provided the investigation team has the relevant IT expertise. This is possibly why two–thirds of survey respondents said they were able to identify the perpetrators.

Over half of the respondents stated that the investigation was performed by internal resources.

Did you investigate the issue, when unearthed?

Source – KPMG India Fraud Survey 2012

How did you investigate the incident?



Source – KPMG India Fraud Survey 2012

Mitigation measures: Not enough focus on physical security

Organisations seem to place a lot of importance on background checks of stakeholders as part of their risk management measures. While most respondent organisations have identified their most valuable data and installed data encryption solutions (as shown below), some respondents do not seem to realise the importance of physical security in the fight against identity theft. One must realise that just having a firewall or other advanced security measures would not be the only deterrent to identity theft. An equally secure physical environment consisting of security measures to limit the physical movement of machines and hard disks as well as preventing the transfer of data on portable devices is important. The recent case of a hard disk stolen from a government department highlights this point[29]. With the upgradation of computers/ mobile handsets and other digital instruments becoming common, the disposal of e-waste is another aspect that needs to be taken care of. Robust protocols around data cleaning and data transfer before disposal on old servers, computers, i-pads, mobile handsets etc. can significantly mitigate the risk of identity theft.

Actions taken to prevent and detect identity theft	Degree of implementation
Conduct thorough background checks on employees, vendors and strategic partners	●
Identify where your most valuable data is and who has access to it	◔
Installed encryption measures for database repositories, laptops and other electronic devices	◔
Establish absolute physical environment security	◐

● indicates >=80%;
◔ indicates >=60% and <80%;
◐ indicates >=40% and <60%;
◕ indicates >=20% and <40%;
○ indicates < 20%

Source – KPMG India Fraud Survey 2012

While it is necessary to have an adequate policy framework, it goes without saying that it should be accompanied by appropriate controls/measures to ensure that such policies are strictly adhered to.

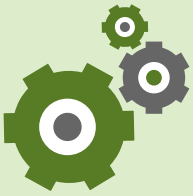
28 Mirjam Staub-Bisang, 'Sustainable Investing for Institutional Investors', March 2012

KPMG View
Tackling Identity theft

Tackling identity theft at an organisational level can be effective with a three-pronged approach.

Training and awareness

Organisations should have a group that collects information relevant to the latest developments in identity theft and shares it within the organisation. Periodic training (online and class room based) can be organised for employees to ensure that they can differentiate between real and fake communication. Case studies detailing instances of identity theft within the organisation or those reported by the media should be shared with employees so that they are aware of the vulnerabilities.



Testing internal process controls

Internal controls in an organisation are only as good as the last time they were breached. Companies must identify all processes and attempt to breach these controls. Putting on the fraudster hat can help identify vulnerabilities in the system. At the very least, there must be a two-level check every time a process change occurs.

Audit and reviews

Spot audits of employee machines can help identify any red flags that indicate identity theft. This way the employee is also alert to the risk of identity theft and will be serious in his outlook towards it.

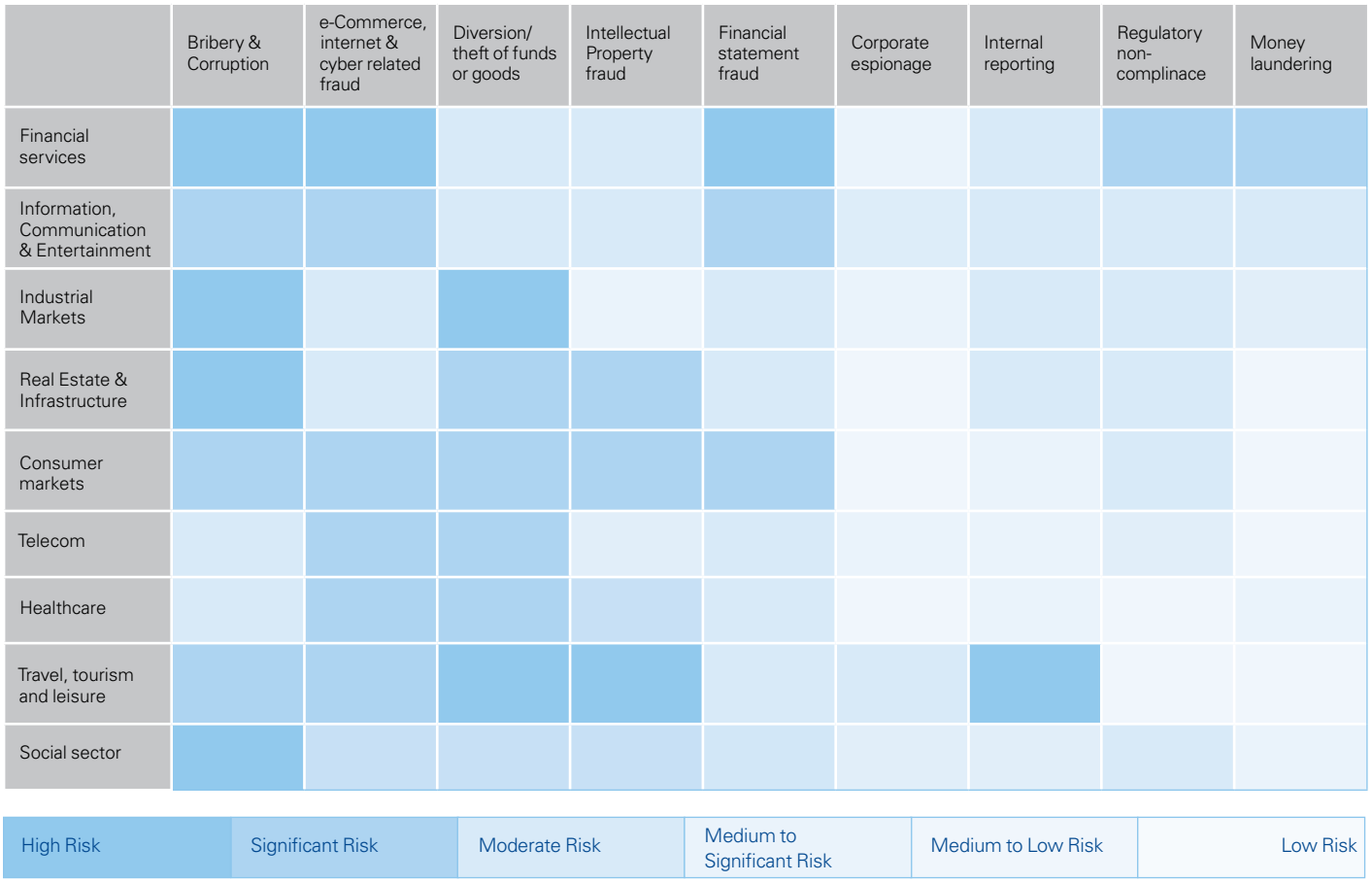
29 http://www.indianexpress.com/news/hard-disk-stolen-from-home-ministry-computer/897468/

Similar trends, different manifestations

Sector perspectives on emerging frauds in India

Our survey results highlight the fact that some sectors are more vulnerable to technology related frauds whereas others are prone to more conventional frauds especially at the process level. There are a range of other unique factors that make each sector more susceptible to a specific type of fraud. For instance, the presence of multiple stakeholders and increasingly complex supply chains makes industrial markets more vulnerable to the risk of diversion/theft of funds or goods. Frauds like bribery and corruption are more prevalent in real estate, infrastructure and industrial markets sectors due to the widespread practice of exchanging kickbacks to obtain the large number of requisite approvals. The sector-wise heat map provides a detailed look into frauds specific to sectors.

Sector-wise fraud risks heat map



Source – KPMG India Fraud Survey 2012

In the subsequent section, we have provided key findings and our point of view for six sectors such as telecom, information & entertainment (IT/ITES), pharmaceuticals, financial services, consumer markets and real estate & infrastructure sectors.

Telecom Sector

Signalling traditional frauds

Key findings

- Around 89 percent of respondents from the telecom sector said their organisations had experienced frauds in the last two years
- Major frauds read, heard or experienced in the sector are:
  - Bribery and Corruption
  - Diversion/theft of funds or goods
  - e-Commerce, internet and cyber related frauds
- Whistle-blower/ ethics hotline, data analytics and anonymous call/ letter / tip off are amongst the top three channels to detect fraud
- After the detection of fraud, 86 percent indicated that disciplinary action was taken against the fraudster and 79 percent suggested that they implemented new or changed existing controls
- To detect and prevent emerging frauds, about 54 percent of the respondents from the telecom sector indicated that they have set-up a dedicated/separate fraud investigation unit. An equal number have also implemented a whistleblower mechanism/fraud reporting hotline.

KPMG View – Procure to Pay cycle frauds rule the roost

Telecom companies (Telcos) operating in multiple geographies amidst evolving technology, services and regulatory environment face a complex set of challenges and risks as they grow their business. Fraud is one of the biggest risks that companies face while battling declining ARPUs (Average Revenue per User), margin pressures and other growth related challenges.

Fraud primarily occurs due to weak internal controls as the Telco business and its leaders are focussed on gaining market share by faster rollout of their networks, launching innovative user services to stay competitive amidst changing technologies and working on new business models to combat declining operating margins. These areas occupy the top management mind space and take away their focus from internal controls, thus making the sector vulnerable to fraud.

According to a global survey by the Communications Fraud Control Association (CFCA), it is estimated that annual fraud losses impacting the revenue (order to cash) cycle of the telecom sector are around USD 40.1 Billion. This is roughly two percent of global telecom revenues. Additionally, Telecom sector respondents to the KPMG India Fraud Survey 2012 have indicated that the sector also faces significant risks from asset misappropriation, fraudulent financial reporting and other frauds in the Procure to Pay cycle.

Unlike most other industries, fraud not only impacts the Telcos but is also directly detrimental to customers' interest. For example, a Telco customer suffers when a fraudster, taking advantage of the poor identity checks at the Telco, is able to use the Telco network for voice/ data connectivity and the bill has to be footed by the customer. This problem is worsened in case the Telcos have mobile money offerings. In such a situation, the customer also stands to lose his mobile money balance. This is typically how "SIM swap" frauds also manifest.

Telcos, both in India and abroad, are gradually taking cognizance of these risks and are adopting some of the following best practices as part of their anti fraud programmes:

- **Social media monitoring:** Fraudsters are using social media to communicate and misuse any existing gaps in Telco networks – whether it is billing or other network related gaps. Further, some fraudsters even float websites luring the public with low or free call rates and other features. To combat this, companies should proactively monitor social media to identify and block any network related gaps, and premium number ranges and sites that result in unintentional calling by subscribers only to find that they have been duped. Additionally, they could also proactively educate their subscribers to not fall prey to such schemes.
- **Setting up a Fraud Control Unit (FCU) that utilises data analytics to identify fraudulent trends:** Telcos have started considering implementation of FCUs by setting up dedicated teams who use pre defined data analytics routines to continuously monitor voluminous data - both within and outside their ERP- to proactively identify red flags that could prevent fraud related losses. This is specifically being used in Telcos to identify fraudulent patterns in the Procurement process, Commissions Payout process, Accounts Payable process etc.
- **Utilising sector focused forensic experts:** Telcos can deploy resources with specialist forensic skill sets to deal with Telecom specific frauds/ issues such as subscription frauds, unauthorised use of network, leakage of sensitive information, interconnect billing problems, misconduct in award and execution of large scale outsourcing contracts etc.
- **Strengthening controls around customer identification:** Stringent Know your Customer (KYC) norms and de-dupe checks based on available patterns are being implemented to detect impersonators that intend to defraud the Telco by assuming false identities and using the network without any intention to pay for it.

Telcos need to follow a two-pronged strategy to combat frauds. This should consist of setting up a Fraud Control Unit to proactively monitor transactions in processes that are more vulnerable to manipulation and simultaneously adopt a co-sourcing model with external sector focussed forensic experts to effectively deal with frauds, identify suspect/s and modus operandi with evidence, so that commensurate action can be taken by the Telcos which then acts as a deterrent for the future.

IT/ITeS

With opportunity comes threat

Key findings

- Around 59 percent of respondents from the information and entertainment sector suggested that their organisations have experienced frauds in the last two years
- Procurement, Sales and distribution, and Inventory are amongst the most vulnerable processes to fraud risks for this sector
- Both management and non-management employees along with external parties (vendors/agents) have been rated as most susceptible to committing fraud
- Post the detection of fraud, 63 percent indicated that they implemented or changed existing controls and 61 percent suggested that disciplinary action was taken against the fraudster.
- To detect and prevent emerging frauds, around 68 percent respondents in the sector have suggested that they implemented a whistleblower mechanism/fraud reporting hotline whereas 54 percent have implemented employee and third party stakeholder due diligence
- In order to familiarise with emerging frauds, corporates in this sector are challenging business processes on a regular basis aiming to unearth gaps in controls (86 percent) and relying on regulatory circulars/ communiqué to get familiar with emerging fraud (59 percent)

KPMG View – New risks emerge

The looming threat of recession, weakening rupee, and the decreasing outsourcing opportunities have brought Indian IT/ITeS firms under pressure, raising questions over their ability to deliver consistent results. Consequently, their guidance, actual performance, and other press releases / statements are now more closely scrutinised by the market. This pressure to perform and meet expectations has increased the risk of fraud in the sector.

The areas most vulnerable to fraud are recruitment, data theft and procurement. Recruitment frauds can take many forms - existence of ghost employees in the company records, collusion with recruitment consultants to recruit otherwise unsuitable candidates in exchange for kickbacks, recruiting employees with fake credentials, unauthorised representation of the organisation in colleges and issuing of fake job offers. Data theft in the sector has traditionally been restricted to employees sharing confidential information with outsiders in exchange for money or gifts.

In addition, our survey indicates three emerging vulnerabilities for the sector.

1. Bribery and corruption

The scale of operations for IT/ITeS companies is large. On an average, the sector recruits over 100,000 people every year. To keep pace with the expansion, companies constantly seek new infrastructure. While leasing facilities continues to be the preferred model for small and mid-sized firms, large IT/ITeS companies now prefer to own facilities. This exposes them to bribery and corruption risks in areas such as land clearances, construction, procurement, interior designing, statutory licenses and facilities management.

Moreover, as opportunities for bagging business from the private sector in US and Europe have reduced due to the recession, the government sector in these regions is emerging as a bankable target for IT/ITeS companies. Gifts or facilitation payments made to win business from governments may impact IT companies negatively due to their presence or their listing in UK/ US. Non compliance with anti-bribery and corruption laws such as the UK Bribery Act and the US Foreign Corrupt Practices may debar IT companies from doing business with these governments.

2. Data theft leading to Intellectual Property Infringement

Data theft (including code theft, modification or deletions of system/ application logs and cyber crime) is increasingly playing a key part in the larger plan in attempts to infringe on intellect property (IP). Although maintaining common login IDs and passwords have been restricted to a large extent, instances of password sharing over email continue. Together these instances contribute to IP theft and need a different level of protection than just having layers of firewall.

3. Risks from channel partners

Sales and customer support are some vulnerable areas where manipulations can happen in the form of inconsistent frequency of product/ service replacements/ upgrades indicating potential fraudulent replacement under warranty, license non-compliance and/or misreporting, as well as channel stuffing and manipulation of sales data resulting in misstatement of revenues.

Channel partners are important as they enhance the scope of offerings in a company. However, if these relationships are not well defined and monitored, these can pose a risk of fraud.

The above mentioned frauds tend to go unnoticed because there is no direct quantifiable financial loss incurred in these areas. Companies must ensure that the tools they deploy cover every extent of organisational data and processes and are continuously monitored. Currently, advanced tools based on data analytics are directed towards monitoring performance, not vulnerabilities. These tools must not be limited to detecting exceptions in transactions but also detect exceptions in transaction trends that expose newer frauds.

Pharmaceuticals
Swallowing the bitter pill

Key findings

- About 54 percent of respondents from the pharmaceuticals[30] sector believe that their organisations have experienced frauds in the last two years
- Procurement, Sales & Distribution and Inventory are amongst the top three most vulnerable processes in this sector
- Around 73 percent of respondents suggested that they implemented new or existing controls post the detection of fraud. Further, 64 percent suggested that they took disciplinary actions against the wrong-doers.
- To detect and prevent emerging frauds, around 62 percent respondents in this sector have established a framework to monitor and ensure compliance of the company's Code of Conduct / Code of Ethics and nearly half of them have implemented a whistleblower mechanism/fraud reporting hotline.

30 Respondents from the Pharmaceuticals, FMCG and industrial markets were grouped under 'Industrial Markets'. The findings may not be representative for each individual sector.

KPMG View –

Regulatory spotlight on compliance drives focus away from growth

While the US continues to be the largest pharmaceuticals market with a size of USD 320 billion[31], due to the economic downturn, most players are adopting cost cutting measures, such as outsourcing to cheaper markets and reducing R&D spends, to remain competitive. Further, approximately USD 135[32] billion worth of drugs are expected to go off patent in the coming years and there is decline in R&D productivity among large players. Given this situation, companies in the sector are focusing on the cost effective generic drugs market. The rising number of ANDA approvals indicates that Indian players are well positioned to take advantage of this growing generics market.

While Indian pharmaceuticals companies focus on growth, compliance is taking a backseat. Consequently, regulators are increasing their scrutiny in a number of areas. Therefore, it is important for the industry to manage compliance issues more proactively.

One of the key compliance risks companies face is bribery and corruption. These risks are compounded by the inherent nature of the business ecosystem that has multiple touch points with vendors, middle men and government agencies. Some situations that expose pharmaceuticals firms to bribery and corruption are as follows:

- A majority of Indian hospitals are public hospitals and these are a significant revenue source for drug makers. Procurement teams at these hospitals can manipulate prices in return for kickbacks from pharmaceuticals companies.
- Medical practitioners have been accused of accepting gifts from pharmaceutical companies in return for promoting drugs made by them
- Regulators such as those from the US Food & Drug Authority as well as regional regulatory bodies conduct periodic audits and inspection of the drug manufacturing facilities. The independence of regional regulators can be compromised to provide favorable reports overlooking malpractices.

With the US Department of Justice and the US Securities and Exchange Commission taking the lead in strictly enforcing anti-bribery and corruption regulations by penalizing companies for non-compliance, Indian organisations need to develop robust controls around bribery and corruption.

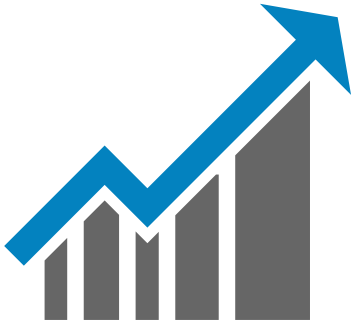
Compliance with current Good Manufacturing Practices (cGMP) is slated to be another area of compliance which severely impacts the reputation of the pharma companies. Various regulatory bodies such as the US FDA, UK Medical and Health Products Regulatory Agency and India's Central Drugs Standard Control Organisation have prescribed a set of measures – the cGMP - to ensure the quality, safety and efficacy of drugs made and marketed in their respective countries.

Non-compliance with cGMP could result in contamination of products and variations in potency and efficacy of the drug, which may lead to death. This in turn could lead to ban on export of products from those facilities. In the recent past, few leading Indian companies have been pulled up by regulatory authorities for failing to meet some aspects of cGMP compliance. This eventually led to a ban on exports of products manufactured at these facilities, resulting in loss of revenue and reputation.

Compliance to cGMPs should be ensured by periodic self assessments by firms and through regulatory inspections. Self inspection helps in identifying any deviations early on so that corrective actions can be taken in time. A good practice to adopt in self inspection is analyzing repeat observations and developing strong corrective and preventive actions for the same. The current expectation of regulators is to evidence implementation of a risk based approach to quality management.

31 ICRA update on Indian Pharmaceutical sector- March 2012

32 Indian Brand Equity Foundation- Cover Story-Pharmacy to the World



Financial Services

Business convenience at a steep cost

Key findings

- Around 59 percent of respondents from the financial services sector suggested that their organisations have experienced fraud in the last two years.
- Major kind of frauds read, heard or experienced in this sector are:
  - Bribery and Corruption
  - e-Commerce, internet and cyber related fraud
  - Financial statement fraud
- External parties (Vendors/Agents / Business Associates), and non-management employees (managers & below) are ranked most susceptible to committing fraud in the financial services sector.
- 76 percent of respondents suggested that they implemented new or changed existing controls after the fraud was detected. Further, 72 percent suggested that their organisations took disciplinary action against the fraudsters.
- To prevent and detect emerging frauds, key measures implemented by organisations include establishing a whistleblower mechanism/fraud reporting hotline (64 percent), introducing process-specific fraud controls (59 percent) and setting-up a dedicated/fraud investigation unit (56 percent).

KPMG View – Technology increases fraud risks

Globally, the last few years have witnessed some unique fraudulent events in the financial services sector such as Ponzi schemes, insider trading, LIBOR rigging scam and more recently money laundering and sanctions non-compliance activities by global banks. These events have led to significant regulatory actions and interventions through legislations. The global governance framework too has been continuously evolving and the trickledown effects are being felt in the Indian financial services sector as well.

KPMG India Fraud Survey 2012 has identified financial services as being the most vulnerable to fraud, whether it is known frauds such as bribery and corruption, or emerging frauds that are technology dependent such as internet banking and mobile banking frauds. Financial sector frauds are becoming complex, their incidence geographically wide spread – many a time perpetrators of internet based frauds and data theft are outside the jurisdictions where fraud is committed – and the quantum of fraud rising. Recent statistics indicate that the quantum of fraud in the Indian Banking sector in 2010-11 was INR 3,799 crore as compared to INR 2,017 crore in 2009-10[33]. The insurance sector also has its share of frauds in the form of fraudulent claims which are bleeding many general insurance companies, while mutual funds are facing flak on issues related to front running.

With greater technology integration in the financial services sector, there are greater challenges. New service delivery platforms like mobile and social media are becoming interfaces between financial institutions and customers, revolutionising the way financial services are delivered. However, with these new platforms comes the challenge of providing a secure environment for customers to conduct transactions. Hostile software programs or malware attacks, risks of phishing, Vishing (voicemail), SMSishing (text messages), Whaling (targeted phishing on High Networth Individuals) and theft of confidential data are all real threats if a secure environment is not established.

Additionally, money laundering and terrorist financing (ML/TF), and tax evasion are also issues plaguing the financial services sector. Recent FATF[34] recommendations indicate that Indian firms would have to set up a comprehensive framework for compliance that includes identification of beneficial ownership and key influencers for an entity. This will also increase the levels of monitoring, diligence and remediation activities carried out by the sector.

Other regulations like the Dodd-Frank Act which prohibits banking entities from any transaction or activity that may involve or result in a material conflict of interest for banking entities, or Foreign Account Tax Compliance Act (FATCA) that prevent offshore tax evasions by US citizens with extra-territorial jurisdiction, are being enforced, which will impact Indian financial institutions even as they grapple to understand these laws.

From a regulatory perspective, Indian regulators such as RBI, IRDA and SEBI have been tightening scrutiny and increasing enforcement. We recently saw 46 banks being fined for non-compliance to AML[35] requirements and insurance companies being fined by IRDA for violation of norms relating to payment of commissions to corporate agents and brokers. SEBI has also set up a Forensic Accounting Cell to investigate potential market manipulation issues. This detailed scrutiny is expected to continue and one can see higher number of sanctions and hefty fines for non-compliance.

Financial services firms can mitigate some of these risks by adopting international best practices that include:

- Conducting yearly risk assessments to identify potential fraud risk prone areas and developing specialised financial crime prevention skills to deter frauds. This should consider global compliance requirements also.
- Employees should be trained and equipped with relevant skills and knowledge about recent fraud modus operandi. They must also be informed of whistleblower channels available to them to report any instances of fraud, misconduct and non-compliance.
- Monitoring channels like social media to gather intelligence and act on early warning signs
- Building an effective Know Your Customer (KYC) framework to prevent any abuse of customer rights and fraudulent transactions

33 CBI address to the CVC - http://articles.economictimes.indiatimes.com/2012-08-07/news/33083590_1_bank-fraud-public-sector-banks-cbi

34 FATF – Financial Action Task Force (FATF) is an inter-governmental policy making body whose purpose is development and promotion of policies to combat money laundering and terrorist financing threats

35 http://articles.economictimes.indiatimes.com/2011-07-11/news/29758455_1_small-banks-aml-apex-bank

Consumer and Industrial Markets

Trust killing the business

Key findings

- 44 percent of the respondents from consumer markets sector suggested that their organisations have experienced frauds in the last two years.
- Major kind of frauds read, heard or experienced in this sector are:
  - Bribery and corruption
  - e-Commerce, internet and cyber related fraud
  - Diversion/theft of funds or goods
- Procurement, finance/payments and inventory have been identified as the most vulnerable processes to fraud risks.
- After the fraud was detected, 81% of the respondents suggested that they implemented or changed the existing controls. Further, 71 percent of the respondents suggested that their organisations have taken disciplinary action against the perpetrators.
- 76 percent of the respondents from the sector suggest that to familiarise themselves with the emerging fraud they challenge business processes on a regular basis aiming to unearth gaps in controls.
- In order to detect and prevent emerging frauds, 65 percent of the respondents suggested that their organisations have implemented a whistleblower mechanism/ fraud reporting hotline. Further, 59 percent of the respondents have introduced process-specific fraud controls.

KPMG View – Firms can no longer discount threat

Consumer and industrial markets (CIM) companies have been the bed rock of modern Indian industry. They have been around for decades and have various anti-fraud governance frameworks. Some have evolved legacy systems and see them as being effective to counter fraud today, while others have re-engineered these frameworks to keep pace with the times, business complexity and scale of operations. Few companies have very sophisticated continuous audit and monitoring frameworks with complex routines built-into them, which alert the organisation to imminent fraud. Although at the very least, a rudimentary anti-fraud framework is in place in the sector, we are often surprised with the extent to which many CIM companies function along a trust-based framework, as opposed to one driven by checks and balances.

The proliferation of technology and the extent to which transactions have grown, both from a volume and value perspective, makes one wonder if anti-fraud protocols in most CIM companies are geared to handle the risk of fraud and misconduct that most organisations face today.

This is reflected in our survey findings wherein nearly half of the respondents belonging to the CIM sector highlighted that they had suffered fraud in the last two years. Does this mean that the other half did not suffer from fraud, or was it perhaps a matter of not having detected fraud due to inadequate detective controls? We cannot be sure as no company is immune from the scourge of fraud.

The survey also indicates that many CIM businesses suffered a large number of small value frauds. In our experience, fraudsters are good risk managers and tend to first test the system with small value frauds, before they graduate to larger, more complex schemes. The size and geographical spread of most CIM sector companies, poses a unique challenge, where distributed operations mean diluted scope of control and oversight. Hence, it is paramount that anti-fraud systems and controls need to be robust.

Many frauds that we have investigated in the CIM sector over the last two years have either involved senior management or external parties; and in a few cases both have colluded to defraud companies. This trend is growing as procurement (a function where maximum collusion is possible) has been identified as high risk area by CIM sector respondents in our survey.

In addition to this, CIM companies are exposed to frauds and misconduct in areas as diverse as bid rigging in procurement, sales and distribution related frauds, recruitment frauds, inventory shrinkage and theft related issues, logistics related frauds for movement of goods, expansion of plant related frauds, counterfeiting of their top selling products leading to significant downstream exposure, regulatory risks such as bribery and corruption (both inbound and outbound), fictitious vendors and cash siphoning, financial statement fraud, conflict of interest positions held by employees, intellectual property theft as well as malice spread through social media and other communication channels leading to erosion in market share.

This is a worrying laundry list of fraud risks that many firms are not adequately geared to address. Perhaps companies can consider adopting the two most effective anti-fraud mechanisms identified in our survey – formal whistleblower mechanisms and fraud risk triggers in the transaction control framework. Some companies in the sector have started adopting these measures and there is scope for others to follow suit.

The Indian growth story, where the consumer base will grow almost ten times over the next 13 years, provides CIM companies untold opportunities for success and riches, yet one large fraud can undo all their efforts. The moot question therefore is are CIM companies doing enough to protect themselves, or is it merely a tick in the box? It is about doing enough to withstand the onslaught of scrutiny, both regulatory and peer, when the chips are down. The aim should not be to baseline oneself along the least common denominator.

Real Estate and Infrastructure

Growing through crony capitalism

Key findings

- 67 percent of respondents from the real estate and infrastructure sector suggested that their organisation has experienced fraud in the last two years.
- Bribery and corruption is perceived to be the most read/heard or experienced fraud by an overwhelming 91 percent of the respondents from the sector.
- Respondents from the sector have rated management employees (senior management and above), external parties (business associates and vendor/agents) as most susceptible to committing fraud.
- 87 percent of the respondents suggested that disciplinary action was taken against the wrong-doers.
- 74 percent of the respondents suggested that they have implemented or changed the existing controls post the detection of a fraud.
- 55 percent respondents from the sector suggested that they have established a framework to monitor and ensure compliance of the company's Code of Conduct / Code of Ethics to detect and prevent emerging frauds.
- Half of the respondents have implemented a whistleblower mechanism/fraud reporting hotline to detect and prevent emerging frauds.

KPMG View –

Need urgent cleaning up of the foundation

The KPMG India Fraud Survey 2012 has confirmed the public sentiment of infrastructure being perceived amongst the most corrupt sectors in the country today. This perception has been strengthened thanks to a number of scams unearthed in the last two years involving companies in the sector having dubious links with members of political parties. Such scams have exposed the irregularities in the sector operations . The multitude of scams is because the sector is characterized by complex sector regulations, large number of contractual relationships, involvement of a large number of government agencies for approvals/ clearance, and significant political involvement during the entire project life cycle.

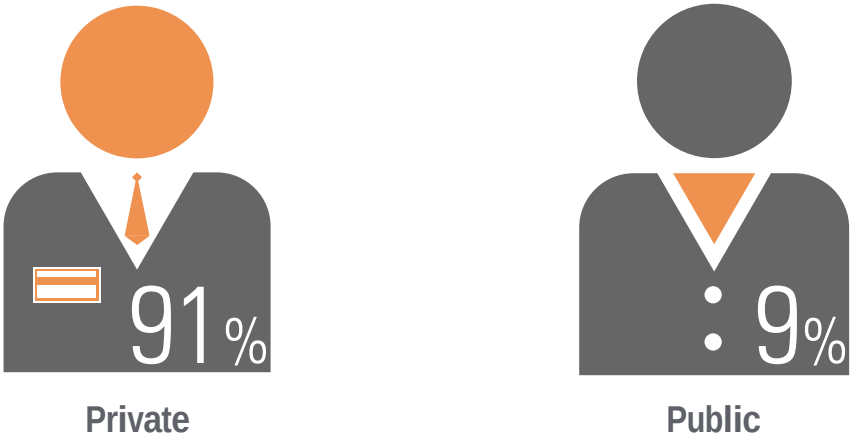
Infrastructure projects face a higher degree of public scrutiny owing to their impact on the public. Recently, the Comptroller and Auditor General of India (CAG) came out with its observations on NELP blocks, coal block allocation, the Adarsh Housing Society allocation of flats, approval of PPP model of operations in an Airport and many other such matters. The focus of these reports has primarily been the decision making process of the Government. The lack of transparency and inconsistency in decision making by government departments, combined with political interference and possible favouritism, makes bribery and corruption a rampant issue in the infrastructure and real estate sector in India. These risks are highest during the pre-construction (land acquisition, environment clearance, clearances from other local bodies, pollution control boards etc.) and construction stages of a project and companies often resort to unfair means to gain an advantage while competing for business. With the government and private parties set to invest USD 1 trillion to create much needed infrastructure in the country, such malpractices not only result in poor quality of projects endangering public safety but also make it difficult to attract international capital.

The government has taken cognizance of this and is moving towards a more robust governance structure within its various departments, particularly keeping in mind the requirements of the infrastructure and real estate sector. Various legislations like the Prevention of Corruption Act (amendment) Bill (2008), the Whistleblower Protection Bill (2010) and Prevention of Bribery of Foreign Public Officials Bill (2011), are all aimed at significantly curbing the menace of bribery and corruption and will benefit the sector if enforced stringently. These legislations are likely to provide a robust legal framework that needs to be backed by strong enforcement to foster an ethical environment for doing business. Further, transparency in the decision making process of such organizations/ departments through full public disclosures will also go a long way in creating confidence amongst investors/ entrepreneurs.

Private enterprises too need to showcase their commitment to this ethical business model by ensuring transparency in decision making and creating a zero tolerance culture. Professionally run organisations with a robust governance model have been able to successfully attract funding, expand their business and gain competitive advantage. Companies can make a start in this direction by aligning their value systems, business vision and internal processes and controls. In our experience, this is usually not done, especially as the company starts to grow. This is made even more difficult as companies tend to change their business models to adjust to the volatile business environment, resulting in weaknesses in the ethical frameworks originally established. As a result, controls originally put in place become outdated and inefficient at tracking any fraud and/or malpractice. Use of technology and continuous monitoring can help the situation, but only to some extent. A re-look at the business foundation and continuous evolution of the control and monitoring framework is the need of the hour.

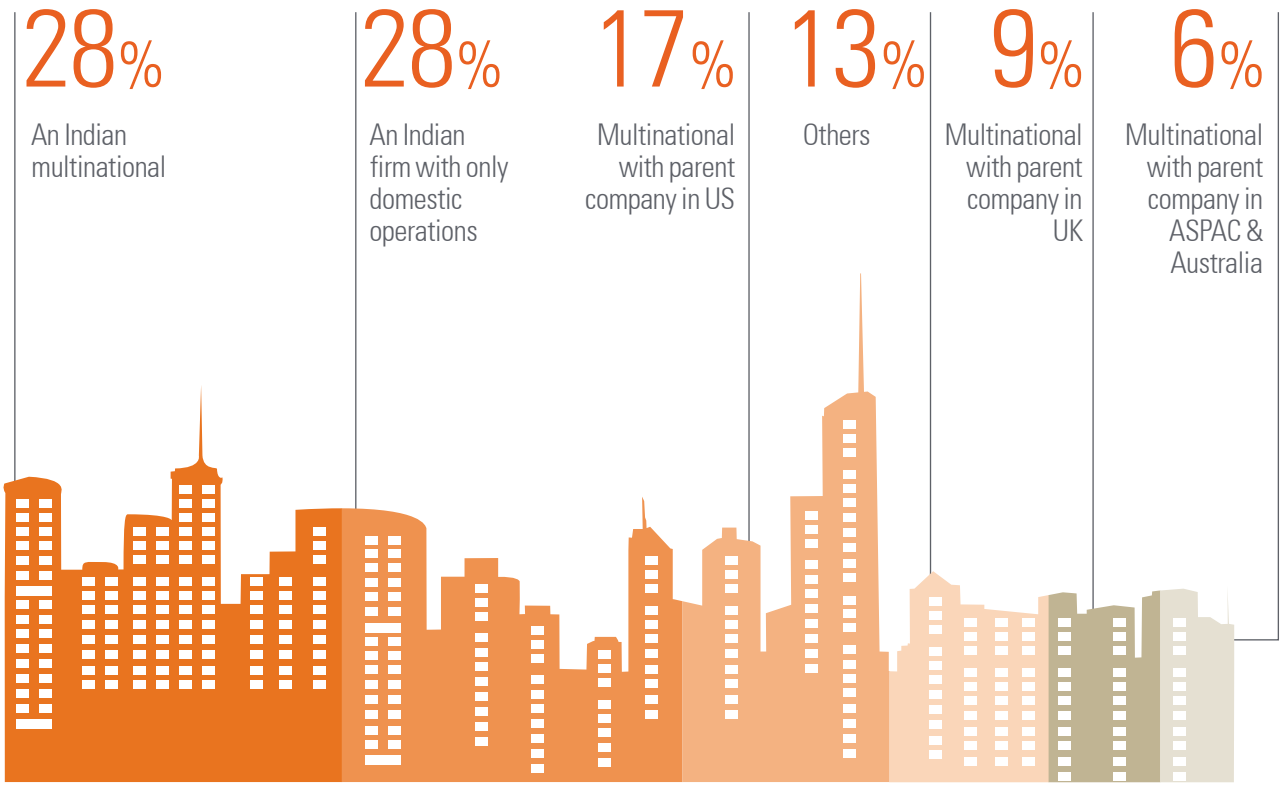
Profile of Respondents

Profile of respondent organisations (Private/Public)



Source – KPMG India Fraud Survey 2012

Profile of respondent organisations (Indian/Multinational)



Source – KPMG India Fraud Survey 2012

Industries that respondents represent

30%
Financial services

20%
Information and entertainment

16%
Industrial markets

11%
Real Estate and infrastructure

9%
Consumer markets

6%
Telecom

4%
Healthcare

2%
Travel, tourism and leisure

1%
Social sector

Source – KPMG India Fraud Survey 2012

Annual turnover of respondent organisation

9%
INR 5001 crore - INR 10,000 crore

12%
INR 500 crore - INR 1,000 crore

14%
INR 1001 crore - INR 5,000 crore

26%
Over INR 10,000 crore

39%
Under INR 500 crore

Source – KPMG India Fraud Survey 2012

Profile of respondents

8%
Ethics officer/ Risk officer

12%
CEO / Managing director

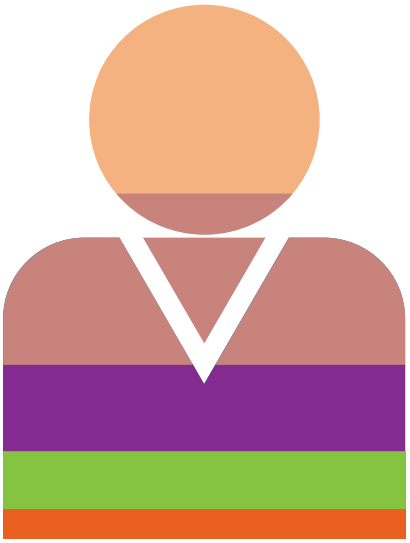
10%
Head of Internal audit

28%
Chief financial offier/ head of finance

42%
Others

Source – KPMG India Fraud Survey 2012

Employee strength of respondent organisation



35% >5000

32% <500

16% 1001-3000

11% 501-1000

6% 3001-5000

Source – KPMG India Fraud Survey 2012

About the survey

This survey was conducted in the month of June 2012 through an online questionnaire on the KPMG in India website.

Over 1,500 CXOs in India were contacted for this survey out of which 293 responded.

Not all respondents answered all sections of the survey, as most sections were optional. The breakup of respondents answering each section is given below.

Section	Number of respondents
Impact of changing business environment and evolving regulatory frameworks on frauds	293
Emerging frauds	193
Bribery and Corruption	86
Identity theft	51
IP Fraud, Counterfeiting and Piracy	42
Cyber crime	45

The survey results of each section have thus been derived from the population of respondents who answered that section. All percentage figures used in a particular section are derived from the population of respondents who answered that section or question and not the total number of respondents who answered the overall survey.

Acknowledgements

Anindita Singh, Archana Venkat, Arpita Pal Agrawal, Balachandra Nadig, Dhritimaan Shukla, Gunjan Uppal, Jayant Saran, Jignesh Desai, Jiten Ganatra, Murali Talasila, Priyanka Agarwal, Rahul Lalit, Rahul Sogani, Ruchi Sharma, Sachin Vichivora, Sandeep Yadav, Shashank Karnad, Suresh Nayak, Suveer Khanna, Uttarayan Sanyal and Vikas Gopal

KPMG in India

Ahmedabad
Safal Profitaire
B4 3rd Floor, Corporate Road,
Opp. Auda Garden, Prahlad Nagar
Ahmedabad – 380 015
Tel: +91 79 4040 2200
Fax: +91 79 4040 2244

Bangalore
Maruthi Info-Tech Centre
11-12/1, Inner Ring Road
Koramangala, Bangalore 560 071
Tel: +91 80 3980 6000
Fax: +91 80 3980 6999

Chandigarh
SCO 22-23 (Ist Floor)
Sector 8C, Madhya Marg
Chandigarh 160 009
Tel: +91 172 393 5777/781
Fax: +91 172 393 5780

Chennai
No.10, Mahatma Gandhi Road
Nungambakkam
Chennai 600 034
Tel: +91 44 3914 5000
Fax: +91 44 3914 5999

Delhi
Building No.10, 8th Floor
DLF Cyber City, Phase II
Gurgaon, Haryana 122 002
Tel: +91 124 307 4000
Fax: +91 124 254 9101

Hyderabad
8-2-618/2
Reliance Humsafar, 4th Floor
Road No.11, Banjara Hills
Hyderabad 500 034
Tel: +91 40 3046 5000
Fax: +91 40 3046 5299

Kochi
4/F, Palal Towers
M. G. Road, Ravipuram,
Kochi 682 016
Tel: +91 484 302 7000
Fax: +91 484 302 7001

Kolkata
Infinity Benchmark, Plot No. G-1
10th Floor, Block – EP & GP, Sector V
Salt Lake City, Kolkata 700 091
Tel: +91 33 44034000
Fax: +91 33 44034199

Mumbai
Lodha Excelus, Apollo Mills
N. M. Joshi Marg
Mahalaxmi, Mumbai 400 011
Tel: +91 22 3989 6000
Fax: +91 22 3983 6000

Pune
703, Godrej Castlemaine
Bund Garden
Pune 411 001
Tel: +91 20 3058 5764/65
Fax: +91 20 3058 5775

www.kpmg.com/in

Contact us

Pradeep Udhas
Partner and Head
Markets
T: +91 22 3090 2040
E: pudhas@kpmg.com

Deepankar Sanwalka
Partner and Head
Risk Consulting
T: +91 124 3074 302
E: dsanwalka@kpmg.com

Dinesh Anand
Partner and Head
Forensic services
T: +91 120 3868 800
E: dineshanand@kpmg.com

Printed in India.