

Deloitte.

India Fraud Survey
Edition I

December 2014
www.deloitte.com/in



Foreword



PR Ramesh

The Indian economy is currently placed at the cusp of revival with visible signs indicating a change in the economic cycle. The new government has managed to improve business sentiment and is giving confidence to investors to make fresh investments across several key sectors such as infrastructure, manufacturing, retail, education, healthcare, and insurance. It has also taken a strong position on the perceived deterrents to investment and growth, such as bribery and corruption, and other unethical business practices, by promoting good governance and enacting legislations to curb such malpractices. While stakeholders are closely observing how these measures will translate into growth for the Indian economy, there is also likely to be unprecedented scrutiny on corporate India's business processes. The Companies Act 2013 will clearly raise the level of governance standards as also increase the monitoring of fraud vulnerability of organisations.

In the past, corporate India has experienced periods of high growth accompanied by challenges in managing certain areas of the business. This was essentially on account of a lag in the development of internal processes and controls, as also relatively less focus on compliance. To benefit from the changing economic conditions, corporate India needs to focus on building a strong backbone of ethical business practices along with a robust framework of compliance and internal controls. Further, over the last few years, we have seen the advent of new age businesses, such as e-commerce, occupy a prominent position in the Indian business landscape.

Additionally, increased use of technology in every aspect of business operations has resulted in a new set of dynamics around fraud risk management.

While organizations have made some investments towards mitigating the risk of fraud, the specific measures adopted appear insignificant in light of the requirements of the fast changing regulatory environment, if one considers the findings of the Deloitte India Fraud Survey Report. To help organizations become aware of the fraud risks they can be exposed to, and help them develop a mitigation strategy, there is need for quality guidance. In that regard, the Deloitte India Fraud Survey Report may provide some key insights.

The report discusses the current state of corporate fraud focusing on prevention, detection and response to fraud, profile of the fraudster, role of technology in fraud risk management, and managing new fraud risks such as those from social media, ecommerce, cloud computing and crypto currency. I am hopeful that the findings of this survey report will help corporate India work towards building a robust fraud risk management framework.

Introduction



Rohit Mahajan,
Senior Director & Head
Deloitte Forensic

Is corporate India doing enough? Probably not.

Corporate India is cognizant of fraud, yet more can be done to mitigate fraud risks and comply with regulations that aim to address fraud risks. This is the sentiment reflected in the Deloitte India Fraud Survey Report.

Even as the business landscape changes, companies continue to battle traditional frauds such as diversion of goods, theft and bribery, indicating that existing fraud risk management mechanisms are perhaps dated and inadequately enforced to tackle these frauds. Further, respondents have said that emerging frauds such as social media fraud, ecommerce fraud, cloud computing fraud, and virtual/ crypto-currency fraud did not pose a challenge to their organizations and it appears from survey data that no specific steps are being taken to prevent these frauds. I believe that some of these areas could pose a serious threat to Indian organizations in the future, given the rising use of social media and cloud computing. Therefore, existing fraud prevention mechanisms used by organizations need to consider the threats posed by these fraud risks.

Such a need is further complemented by the requirements outlined in the Companies Act 2013. While Corporate India grapples with the right approach suitable to their respective organizations, a comprehensive approach to strengthening fraud prevention will prepare organizations to move into the next level of business maturity. A check-in-the-box approach wherein

the entire effort is looked as compliance cost rather than as a business driver will impact the sustainability of business over the long run in an increasingly global environment.

A change in mindset is needed to view fraud risk management as a proactive ongoing effort that will, over the long term, create robust internal controls and other mechanisms to mitigate the risks of fraud. Organizations will need to make investments to put in place systems and processes aimed at curbing fraud and meeting compliance requirements.

I believe that, while regulations such as the Companies Act 2013 can provide sufficient impetus for organizations to change their mindset about proactive fraud risk management, self-realization of the risks to reputation and business can be a better driver of this action.

It gives me immense pleasure in bringing to you Deloitte India's first comprehensive fraud survey report. This is our attempt to present key trends and developments in regards to frauds risks that Corporate India faces in a dynamic and evolving business environment. I want to thank all our survey respondents for supporting us in this endeavor. I look forward to your feedback.

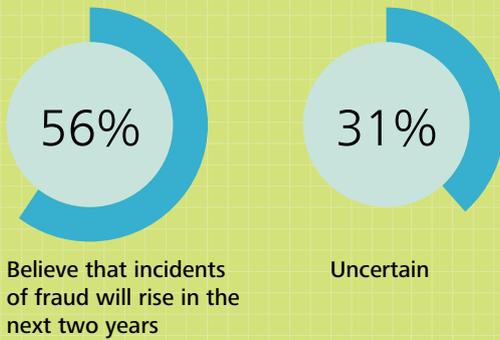


Contents

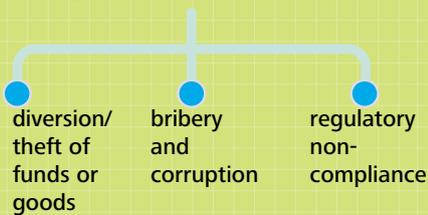
Key findings	6
Section 1: The face of fraud today	8
Fraud continues to be on the rise	9
Preventing and detecting fraud	16
Impact of the Companies Act 2013 on the state of fraud	22
Section 2: Managing the face of fraud tomorrow	27
e-commerce Fraud	29
Cloud Computing fraud	32
Social media fraud	34
Virtual/ Crypto-currency fraud	37

Key findings

Fraud is on the rise



Top 3 frauds experienced by organizations

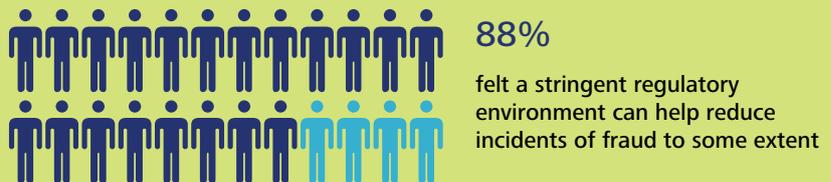


Who is the fraudster?



Senior management identified as most susceptible to commit fraud, whereas external parties were least likely to commit fraud, as per survey respondents.

Impact of Companies Act 2013 on the state of fraud



- Most effective clauses in fighting fraud
 - Mandatory establishment of a vigil mechanism for listed companies
 - Greater accountability on board and directors to prevent and detect fraud

Fraud Detection moving towards maturity

50% felt the Chief Security Officer should be responsible for fraud investigation

75% felt external auditors should be responsible for fraud detection

Top channels



Internal audit review



whistleblower hotlines



IT controls / data analytics

Key actions taken upon fraud detection



Greater awareness around fraud prevention measures

Felt that the Board should be responsible for preventing fraud

>75%

Top 3 processes that every fraud risk management framework should include

59%

regular monitoring/ assessment of fraud risks

56%

conducting due diligence check

50%

the use of proactive forensic data analytics

Limited awareness about technology led new frauds



Social media fraud

69%

Were unsure about this fraud risk, felt there was inadequate guidance in legislation to deal with social media frauds in India



E-commerce fraud

60%

Felt e-commerce was not risky, and appeared not to have comprehensive processes within their organizations to mitigate this fraud



Cloud computing

96%

Claimed their organizations had not suffered this type of fraud

57%

Unaware of any review of compliance and security policies pertaining to cloud computing



Crypto currencies fraud

50:50

Mixed views on the safety of virtual currencies

72%

Virtual currencies were not a part of their organization's strategy

Section 1

The face of fraud today



Fraud continues to be on the rise

The last decade has seen significant coverage of corporate fraud in the Indian media. While the Indian government has passed several laws aimed at curbing fraud,¹ poor enforcement has diluted the intended impact. With the rise of new business models backed by technology, fraud has spawned new variants and seems to be on the rise. Around 56 percent of our survey respondents believe that fraud will continue to increase in the coming years

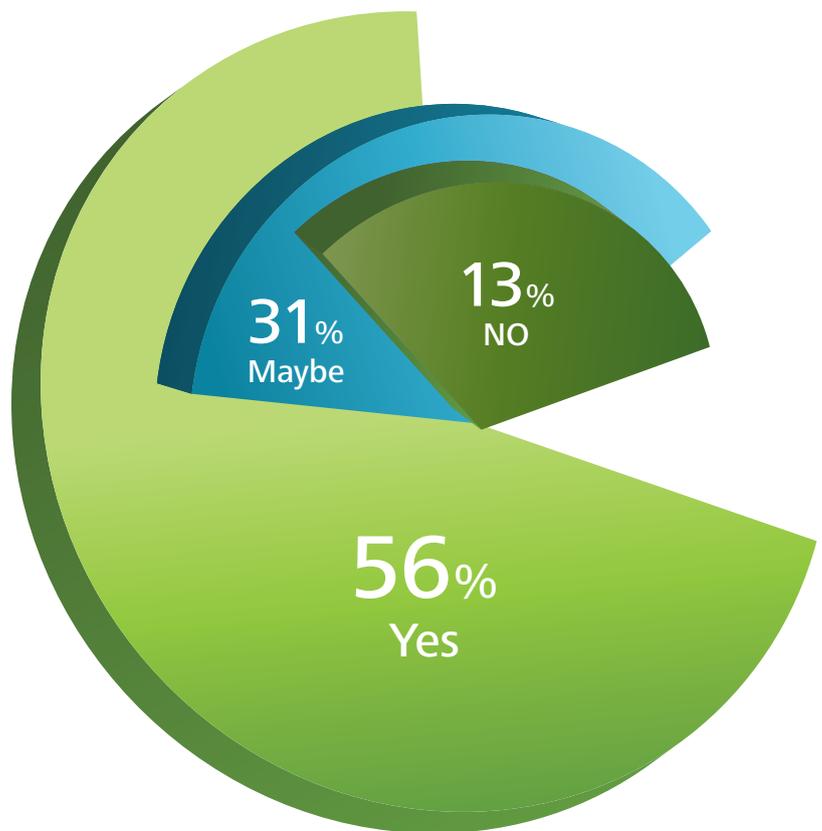
Traditional schemes² dominate the fraud landscape

Despite the extensive adoption of technology by organizations to build global business models, corporate India continues to face challenges in mitigating traditional fraud schemes. According to our survey respondents, diversion/ theft of funds or goods, bribery and corruption, and regulatory non-compliance were the top three fraud concerns faced by their organizations. Further, over 50 percent of survey respondents felt that procurement, sales and distribution functions were most vulnerable to fraud, indicating that greater business exposure to external stakeholders such as vendors, suppliers, customers, and distributors could significantly increase the risk of fraud.

Around 28 percent of the survey respondents have indicated that their organizations did not experience any fraud in the last two years. In our experience, organizations with robust internal controls detect red flags regularly and investigate them for potential fraud. In the absence of red flags or fraud, we would recommend that organizations re-look at their controls and test them for effectiveness.

In our view, insufficient mechanisms to prevent and detect fraud, as well as limited enforcement of internal controls are likely to be the reasons that organizations continue to experience traditional fraud. Specifically in the area of bribery and corruption, organizations have, in the past, considered bribery as the 'cost of doing business', and hence demonstrated a degree of acceptability towards this practice. But with increased scrutiny by foreign regulators, and the Indian government taking a tough stand on bribery by enforcing legislations like the Prevention of Corruption Act while passing judgments on cases, we are seeing several companies taking efforts to address the risk of bribery and corruption.

Figure 1: Do you believe that incidents of fraud will increase in the next two years?



¹ In the last decade and a half India has enacted the following legislations aimed to curb fraud - the Prevention of Corruption Amendment Act 2011, the new Companies Act, 2013, The Whistleblowers Protection Act, 2011, The Right to Information Act, 2005 (RTI), The Information Technology Act 2000 (IT Act), and The Prevention of Money Laundering Act, 2002 (PMLA).

² These are fraud schemes which have been in existence for more than a decade and ones that companies are fairly well exposed to.

Figure 2: Which of the following types of fraud/ misconduct/ noncompliance has your organization experienced in the last two years?



Tackling bribery and corruption

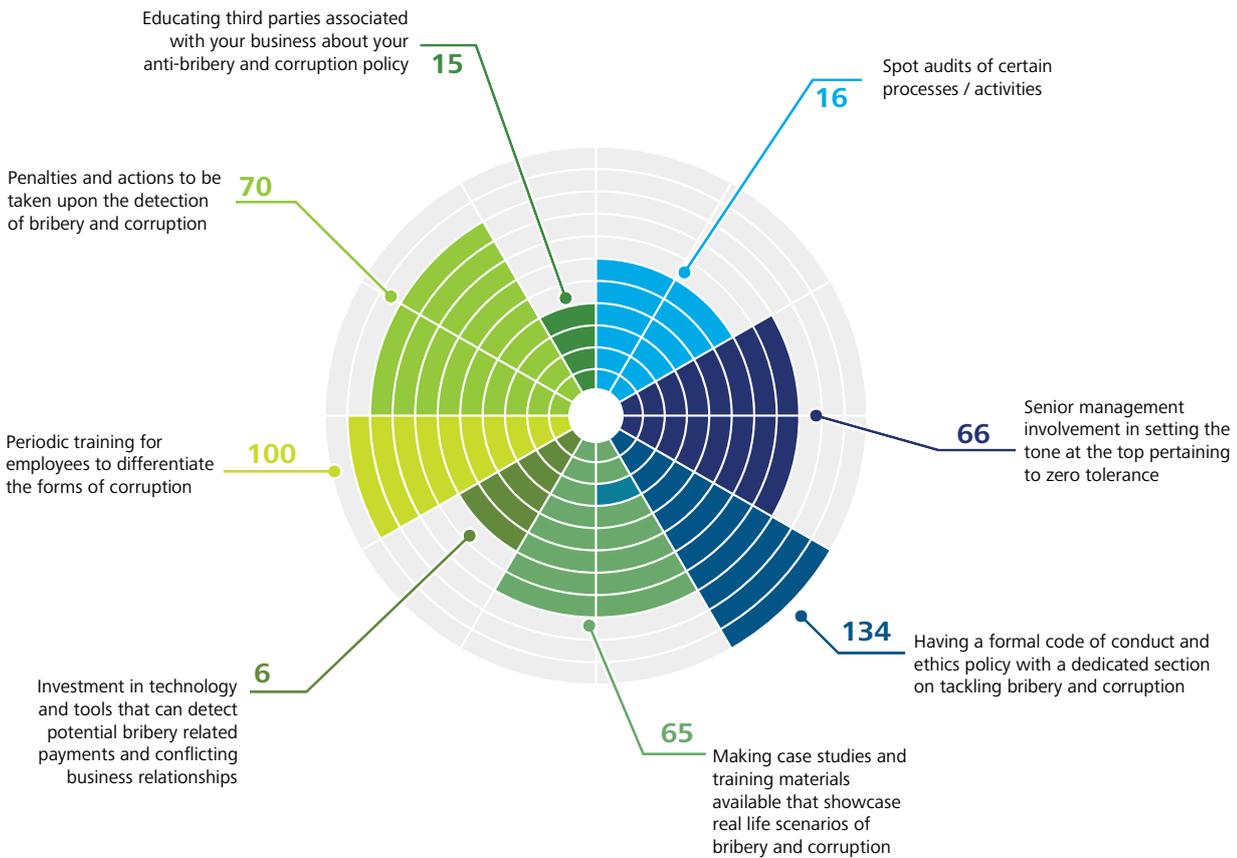
The majority of survey respondents have indicated that their organizations are considering implementing a formal code of conduct and ethics policy with a dedicated section on tackling bribery and corruption, followed by imparting periodic trainings to employees on understanding and dealing with various forms of corruption. This behavior is indicative of the changing attitudes to bribery and corruption in corporate India.

It is believed that the way the senior management deals with external stakeholders (regulators, suppliers, customers etc.) has a strong bearing on how the employees of the organization perceive the business is run. Hence, the tone-at-the-top and actions of the senior management are a critical measure of how successful an anti-bribery and corruption program is/ will be. However, we noted that a relatively small portion of the survey respondents considered this aspect when they wanted to tackle bribery and corruption. Our interpretation is that while, corporate India acknowledges that the process of mitigating the risk of bribery and corruption is ongoing, it feels that policies and procedures may be sufficient guides to help drive positive behavior among employees.

Another interesting finding is that a small portion of the survey respondents considered the need to educate third-parties to tackle bribery and corruption. At the same time, a majority of survey respondents identified tracking the levels of compliance by third-party stakeholders as the key challenge to implementing an anti-bribery and corruption compliance program. While at first glance, these statements appear to be contradictory, it is possible that companies are relying only on internal controls to mitigate the risk from third parties. As organizations mature, we hope to see stringent anti-bribery and corruption compliance measures being expected of external stakeholders, and hence better monitoring of their compliance levels.

Interestingly, a very small number of survey respondents stated that they are investing in tools and technology, especially data analytics, for detecting potential bribery and corruption instances. In our experience, technology is a powerful mechanism to mitigate potential bribery. Globally, we see companies investing in tools to monitor high-risk activities involving functions or individuals working with the government/ vendor organizations. These activities are tracked to identify red flags such as conflicts of interest, complex routing of transactions

Figure 3: Which of the following measures have you considered implementing within your organization to tackle bribery and corruption?

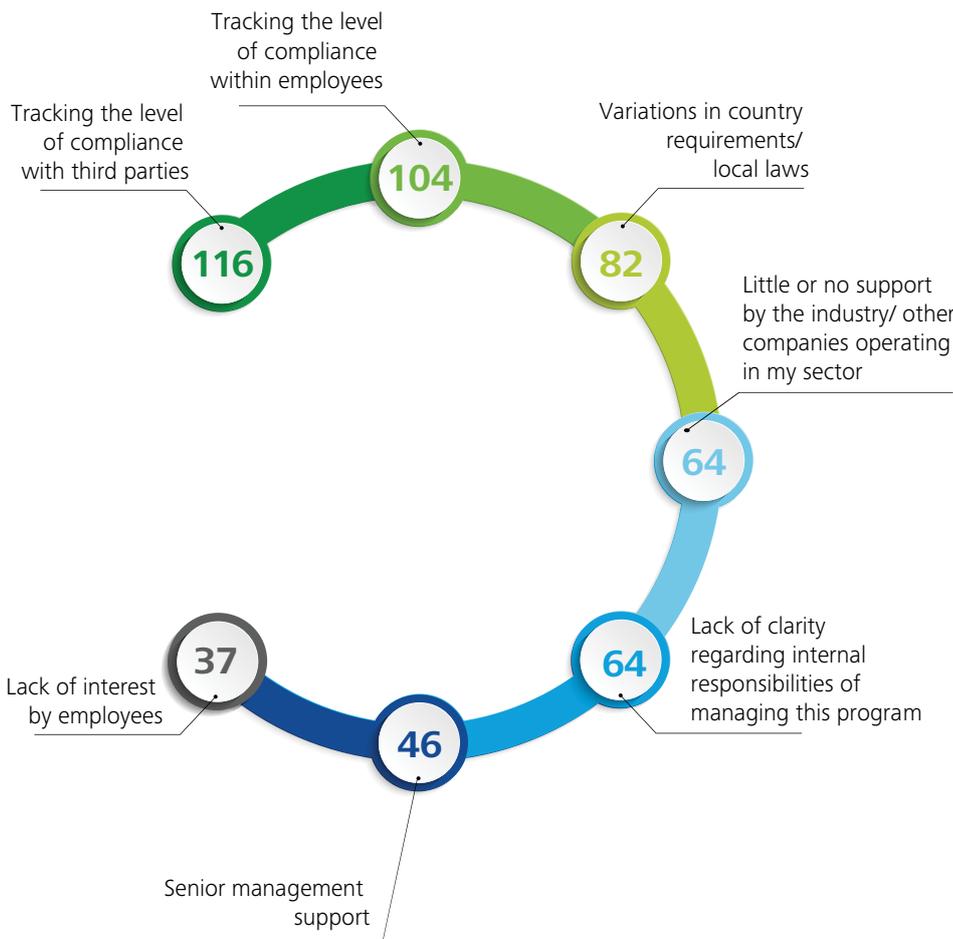


through third parties, mismatched invoices and purchase orders, back-dated contracts, unusually high payments made to counterparties, unusual phrases used for denoting facilitation payments and bribes, as well as mismatched expense claims.

With strong enforcement of global laws, we are seeing Indian companies with global operations demonstrating a zero tolerance culture within the organization. In addition, many industry bodies have set up committees to help organizations identify and adopt good practices to mitigate the risk of bribery and corruption. The World Economic Forum has launched the 'Partnering Against Corruption Initiative' with industry bodies across the world to strengthen business and government collaboration on increasing transparency in business dealings.

Additionally, companies can also look at adopting the OECD convention against bribery as well as international standards such as the UK standard BS10500 or the future ISO standard PC278 to adequately secure themselves against bribery and corruption. The Indian government, on its part, has initiated programs such as e-procurement in select departments with an aim to curb bribery in public dealings. The coming years are likely to see a strong enforcement of Indian legislations in the area of bribery and corruption, considering the recent cases of enforcement of the Prevention of Corruption Act against corporates. With further proposed changes in the Prevention of Corruption Act, the Indian anti-corruption law is expected to become at par with international regulations.

Figure 4: What do you feel are your organization’s top three challenges in implementing an anti-bribery corruption compliance program?



Contributors to fraud

Survey respondents attributed the prevalence of fraud risks to the lack of efficient internal controls/compliance systems, diminishing ethical values and inadequate due diligence of employees/third parties.

In our experience, we have observed that many companies do not spend enough time building robust backend systems to manage fraud risks. While Indian businesses use technology to monitor transactions, there is room for significant automation of processes and controls. Human touch points continue to monitor and manage technological controls. People managing these processes can be compromised or may unintentionally overlook certain aspects of compliance in a bid to focus/support growth.

For instance, during the growth phase, companies tend to put pressure on executives to grow the business, often linking compensation to achievement of business targets. In such instances, compliance and fraud risk management processes tend to get ignored, given the heightened single-minded focus on growth. In light of the socio-economic developments over the years, and the potential for growth in the future, there is a rise in aspiration levels among people. At times, the need to fulfil these aspirations can lead to a tendency to compromise on ethical values. Therefore, we believe it is imperative for companies to invest in developing a robust code of conduct and follow it up with a comprehensive program to ensure that the code is imbibed by employees in their day-to-day business activities.

Survey respondents have also highlighted that inadequate due diligence on third parties is one of the key contributors to fraud. Adequate due diligence that includes understanding the counterparty’s market reputation, relevant experience, business interests and affiliations, financial position, clients served and litigation exposure can help identify the right partners. In addition to undertaking due diligence activities, we also believe that organizations which invest in helping their external stakeholders imbibe and comply with the organization’s values, see better working synergies and reduced risk of fraud.

Profiling the Fraudster

Instances of big-ticket frauds in Indian corporations have historically involved employees, either as perpetrators or as conduits. Survey respondents indicated that senior management employees (senior managers and above) were most likely to commit fraud. However, in our experience all employees are equally susceptible to committing fraud.

The infographic in the next page highlights the types of frauds most likely to be perpetrated across all levels of employees in an organization and the indicative red flags. The table has been developed on the basis of Deloitte India forensic team’s experience of fraud detection over the last couple of years.

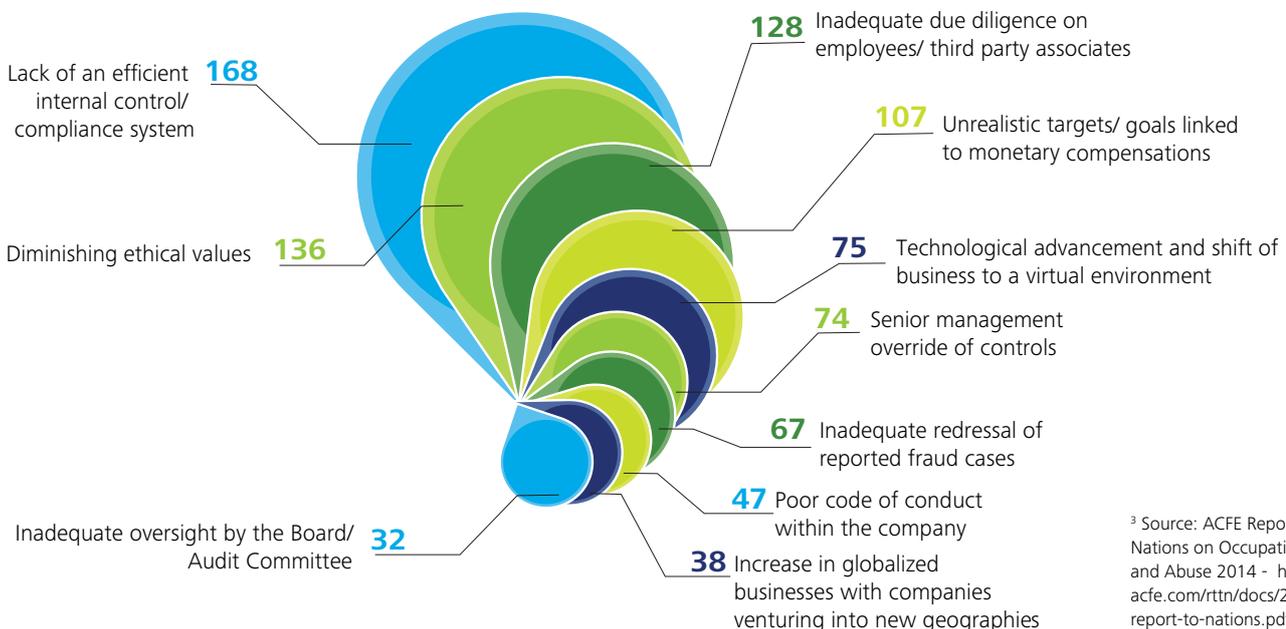
Fraud losses continue to be deceptive

Although large value scams running into several hundred crores of rupees are making media headlines regularly, responses to our survey indicate that perhaps majority of corporate India does not experience even a fraction of that value of loss. Only 3 percent of our survey respondents said they suffered fraud loss of over Rs 100 million. About 38 percent of our survey respondents said that they had suffered no fraud loss and another 23 percent said they were unable to quantify the loss due to fraud.

Globally it is estimated that the average fraud loss in companies is about 5 percent of revenues³. This raises concerns over corporate India’s understanding of fraud loss and the ability to compute it accurately. This, in turn, may result in a lackadaisical approach to implementing fraud risk management measures.

It is important to understand that in addition to the monetary loss from fraud, loss of reputation and credibility can also have severe repercussions for a business – long term ban from conducting business or in some cases, business termination itself. These aspects too must be considered when one thinks of fraud loss.

Figure 5: What do you feel are the reasons that can contribute to fraud?



³ Source: ACFE Report to the Nations on Occupational Fraud and Abuse 2014 - <http://www.acfe.com/rtnn/docs/2014-report-to-nations.pdf>

SENIOR MANAGEMENT

Kind of Fraud most susceptible to commit

Financial statement manipulation – such as inflating or pre-booking revenues / inflating fixed assets / diverting loaned funds to shell companies/ diversion of stock or funds

Indicative red flags to watch out for

- Projecting earnings better than the industry average
- Increase in fixed assets on balance sheet not commensurate with increase in production capacity
- Large Debtors in the balance sheet for a prolonged period.
- Movement of balances between different debtor accounts
- High inventory levels and slow movement of raw material in stock
- Large number of transactions (sale/ purchase or loans) with related parties
- Large loans and advances made to group companies with insignificant operations
- Unrecorded/ concealed liabilities and expenses
- Advanced revenue recognition
- Profits not getting converted to cash

Insider Trading

Indicative red flags to watch out for

- Huge swings in share price before public announcement of confidential information is made such as takeovers, bankruptcy, financial results etc.
- Block sale of shareholding in the firm prior to a key announcement
- Non-disclosure of demat accounts by fund manager

Conflict of interest that may result in noncompliance

Indicative red flags to watch out for

- Undisclosed business interests/ ownership of entities

JUNIOR MANAGEMENT

Kind of Fraud most susceptible to commit

Asset Misappropriation – Petty cash

Indicative red flags to watch out for

- High value payments disbursed from petty cash
- Operational or regular payments (which should ideally be contract/PO based) made from petty cash
- Absence of adequate supporting documentation for petty cash expenses

Data theft/ leakage

Indicative red flags to watch out for

- Suspect works unusually long hours
- Frequent use of personal external storage devices on company machines
- Unusually high usage of personal email accounts in the office
- May not show a propensity towards role change

MIDDLE MANAGEMENT

Kind of Fraud most susceptible to commit

Bribery and Corruption – Procurement fraud

Indicative red flags to watch out for

- Inadequate supporting documentation for the bids
- Similarities in format and content of quotations submitted by multiple bidders
- Most bids are won by a single entity or, more often than not, the winning bid is marginally lower than the L2 bid
- Sub-standard quality or higher rejection rate
- Duplicate entries for PAN, bank account or contact details between employee and vendor master, or within the vendor master
- Multiple vendor codes with different bank account numbers
- Payments made without appropriate invoices
- Vague descriptions in the invoice such as 'out of pocket expenses', 'discretionary expenses,' 'incidental expenses' and 'agent/ consultancy fees'.
- Extensive use of agents/ consultancies that is not in line with industry practices

Asset Misappropriation – Payroll or expense reimbursement fraud

Indicative red flags to watch out for

- Multiple employees mapped to a single bank account
- Contract workers appointed through labor contractors but no statutory details like PF numbers, ESI numbers etc. available
- Minimal absenteeism or huge overtime payments towards contract workers
- Inadequate documentation in support of skill level of contract workers (particularly in case of skill-based remuneration)
- Mismatch in employee records from HR and attendance records based on cards swiped/ biometrics
- Mismatches in ticketing and hotel dates
- Unsupported reimbursement claims, reimbursement claims based on similar invoices, food/entertainment bill claims from city different from city of travel

Market Manipulation such as front-running (applicable to the Fund Management Industry)

Indicative red flags to watch out for

- Unusually high activity observed in trading a few stocks belonging to the client's portfolio
- Movement of stock price around the time a transaction is undertaken by a fund manager
- Sudden improvement in wealth / lifestyle of the employee

Asset Misappropriation - Theft of inventory

Indicative red flags to watch out for

- Mismatches in stock keeping records
Increase in obsolete or written down inventory
- Suspiciously high scrap disposal (frequency/ quantity)
- Sudden improvement in wealth / lifestyle of employee

Preventing and Detecting Fraud

In the past, companies focused on putting in place basic processes and controls to improve operational efficiency, control and oversight. Today, however, there is a further need to implement mechanisms that are specifically aimed at mitigating the risk of fraud, and enabling early detection in the event of an incident.

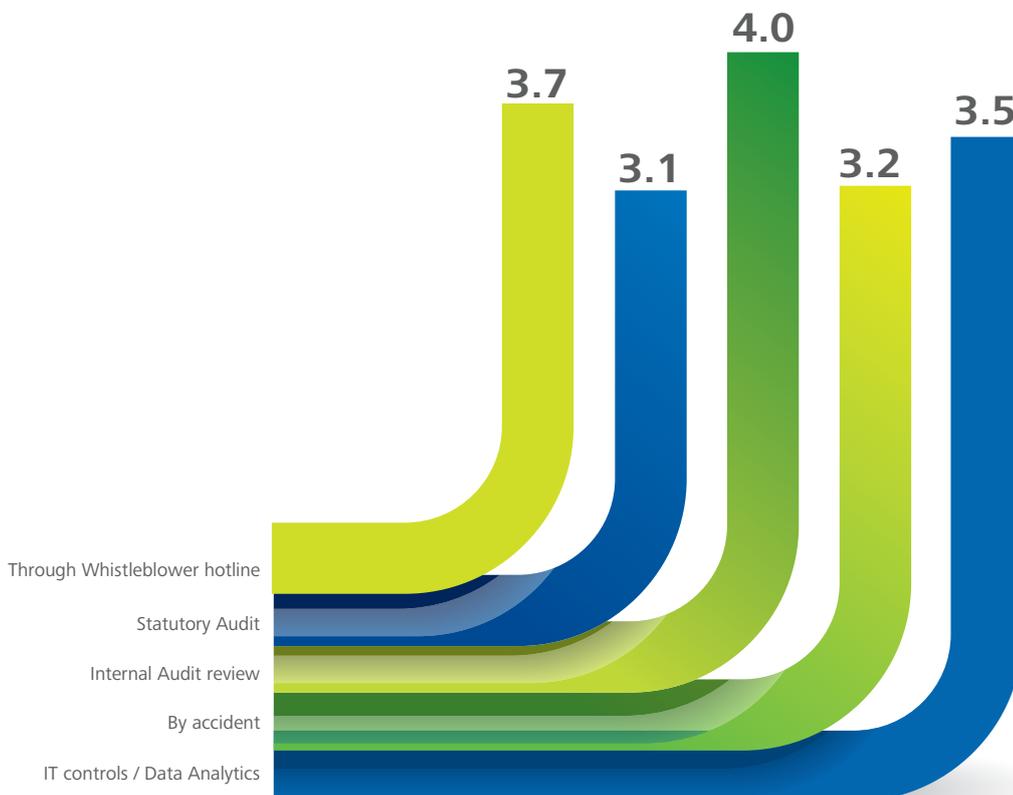
Our survey results indicate that internal audit continues to remain in the top spot as a channel to detect fraud. However, whistleblower hotlines, IT controls/Data Analytics are rapidly gaining ground as fraud detection

Whistleblowing hotlines have proven to be an effective means of fraud detection globally, and form an integral part of a robust fraud risk management framework. Data collected from whistleblowing hotlines can be useful in identifying patterns and trends leading

to potential red flags. However, in our experience, whistleblowing programs in corporate India need greater attention. Currently, whistleblowing programs are implemented either as part of a larger fraud risk management framework, or to primarily meet regulatory requirements⁴, making them relatively ineffective in detecting fraud.

For a whistleblower program to be successful, it needs senior management commitment and an enhanced degree of awareness among employees around the benefits of a whistleblowing mechanism so that they feel comfortable and confident while reporting their concerns through the channel. This can be done through periodic workshops and trainings, and ensuring visibility through internal promotional tools such as posters, screensavers and wallpapers, flyers and giveaways.

Figure 6: How are fraud incidents detected in your organization? (Responses are ranked uniquely from 1 to 6 with 1 being the least common and 6 being the most common practice used to detect fraud. Weighted average of the scores is depicted below).



⁴ Source: Deloitte Forensic’s survey report on whistleblowing programs titled Lead by Example: Making whistleblower programs successful in corporate India, released in 2014 - <http://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-fa-whistleblowing-survey-2014-noexp.pdf>

Figure 7: Using forensic data analytics, which of the following frauds has your company been able to unearth/ detect?



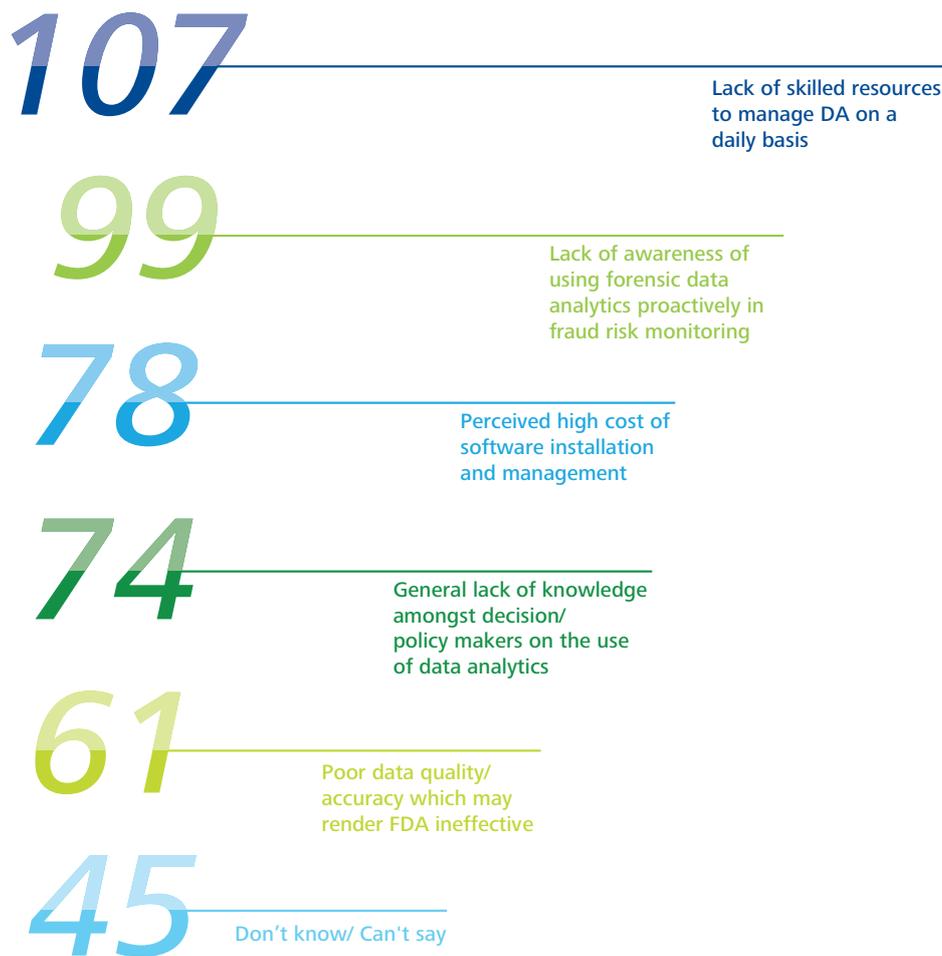
Alongside whistleblower programs, IT controls/ Data Analytics have emerged as a key channel to detect fraud. Apart from measures such as restricted access to online resources and controls over use of external storage devices, organizations are increasingly using Data Leakage Prevention (DLP) software to monitor the movement of data to and from office systems. Further, organizations work with huge volumes of data and it would be difficult to detect any anomalies without the use of data analytics tools that can process such data fast and pick out exceptions. We have, in our experience, observed that effective forensic data analytics can help companies detect at least 11 types of fraud schemes (see figure above).

While forensic data analytics can be used for a periodic diagnostic review to identify any red flags in historical

transactions, it is of greater importance to use these tools proactively for continuous fraud monitoring, which would involve real-time or near real-time analysis of transactions across business functions, so that any misconduct can be identified and controlled before the damage is done.

However, continuous fraud monitoring can be a challenge for organizations that may not have dedicated resources to manage data analytics functions on a daily basis or even understand how to utilize them, as indicated by majority of the survey respondents. That being the case, organizations may not see favorable outcomes pertaining to fraud detection and mitigation, despite investing in analytics tools across a range of processes and functions.

Figure 8: What challenges do you face in the adoption of data analytics techniques in fraud prevention?

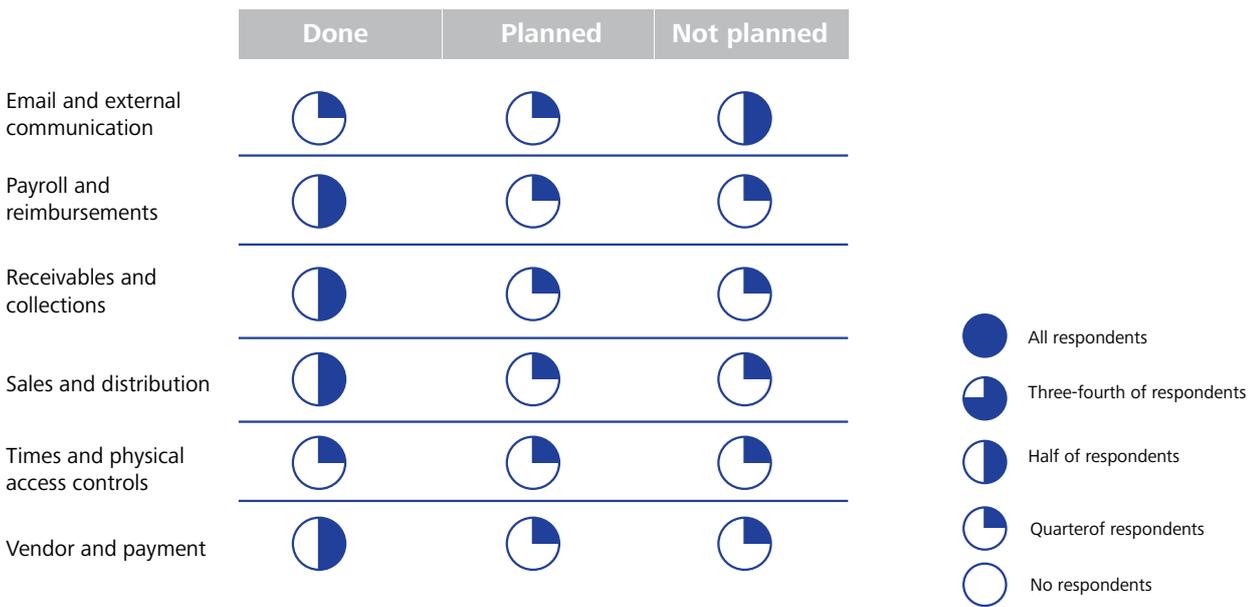


Deloitte Point of View - Leveraging your enterprise software to detect and prevent fraud

As indicated by the survey respondents, the adoption of technology and analytics for fraud risk management among Indian businesses seems to be moderate to high. Yet, on the basis of the responses received, it appears that companies have not had much success in using technology to detect or prevent fraud.

In our experience aligning specific IT controls with fraud risk management processes can possibly improve detection of fraud. Below are some practical tips based on our experience that companies can use to enable better fraud risk management outcomes from their existing technology platform.

Figure 9: Does your organization run proactive data analytics on the following processes to monitor fraud?



- **Logging and maintaining an audit trail of activities**

In our experience, most companies maintain logs more from a system diagnostic and troubleshooting perspective than from a fraud risk management perspective. The retention period for logs should also be determined keeping in mind the fraud risk management requirements. We recommend that a multidisciplinary team with representatives from legal and compliance teams work together to develop a robust log maintenance policy. It is important that analytics should be routinely run on logs, and these logs should be routinely reviewed to identify unusual patterns and red flags.

- **Automated notifications (emails/ text messages) in cases of process overrides**

Well known security monitoring tools can be configured to send automated notifications to designated stakeholders when a particular event is triggered. If configured properly, such automated notifications can help ensure that the right people are notified of control overrides without delay which helps reduce the response time required to contain the fraud risk.

- **Active Threat Monitoring and Management**

Most Enterprise Resource Planning (ERP) systems have Business Intelligence modules that can be configured, depending on the type of business and data inputs available, to generate red flags for deeper enquiry. While there are no universal settings or standard operating procedures for this, we would recommend enabling cross departmental integration of data from systems such as between HR, Payroll, Administration and Finance to ensure a holistic view of fraud risk management.

- **Audio Visual monitoring**

This involves video recording the premises and eventually integrating the video feed with ERP data to cross check details pertaining to transactions. This is commonly done at Toll plazas and retail point of sale counters. For instance, in our experience one of the most common forms of toll plaza fraud include miscategorization of vehicles and therefore the corresponding toll amount charged. With a video feed, cross checking this becomes a lot easier. Globally, audio visual monitoring is believed to increase the 'perception of detection' as employees are aware that someone is watching them, and

therefore they are cautious in their conduct and behavior.

- **Data Leakage Prevention (DLP) software**

Typically DLP software run on key word based routines, filtering out transactions with those keywords. However, we see that fraudsters are working around this issue by encrypting content in a manner that will pass through the DLP software. In some cases, fraudsters also change file extensions to transfer data without it being detected by the DLP software. These issues can be overcome with policy tweaks such as allowing certain emails outside the group domain only if a copy is marked to a particular email id – generally that of a monitoring group etc.

- **Adequate control on devices (employee owned and office owned) containing confidential office data**

All devices containing corporate data should be encrypted to ensure confidentiality, in case the device is lost or stolen. There are software tools that can remotely wipe data from such devices over the network to ensure that data is not used by the wrong people.

Due diligence rising to prominence

In the larger context of fraud risk management, we would like to draw attention to the increasing role that forensic due-diligence is playing. As organizations work with an increasing number of third parties, the risk of associating with the wrong set of business partners can stretch beyond reputational risks, resulting in monetary losses and legal battles.

In India, promoter-investor/partner conflicts are often reported by the media. Companies can, to an extent, safeguard themselves from liaising with the wrong partners by conducting a pre-investment/pre-acquisition forensic due diligence to identify alignment of the potential partner's goals to their own, potential integrity issues or past legal entanglements. Due diligence procedures are also used while recruiting strategic hires like senior management personnel who manage highly sensitive information, and handle roles where their integrity and reliability is of paramount importance. The due diligence in this case is used to verify the credentials, capabilities and integrity of new appointees.

Our investigation experience indicates that contracting/ procurement continues to remain highly vulnerable to fraud risks, necessitating vendor due diligence procedures to understand the independence of the vendor, their capabilities and reputation in the market, as well as identify any adverse information that could affect the relationship between the entities, prior to appointment of the vendor. Adopting a structured approach to due diligence at various points of the business process is therefore a key aspect of an ideal fraud risk management practice.

Deloitte Point of View - Building a due diligence process framework and including it in your fraud risk management plan

Business intelligence ("BI") is a key component of a due diligence program and is an evolving risk mitigation tool. It can be applied both as a pre-emptive strategy for fraud prevention and for generating critical leads when investigating a fraud. In certain situations where access is restricted, an investigation can be conducted through an 'outside-in' BI process.

BI combines examination of information in the public domain with market intelligence gathered through relevant stakeholders to form a comprehensive view on the credentials, reputation, financial strength and business practices of an entity or individual that is the subject of the due diligence/investigation. As part of a due diligence program, BI assists corporations/ individuals to get access to information that can be used to quantify potential risks.

Including a due diligence process as part of the larger fraud risk management plan can help avoid legal complications, costly mistakes and reputational damage. This can help detect the modus operandi of frauds perpetrated by employees and identify the manner in which the suspects have materially benefitted. BI can also help strengthen cases for prosecution by providing leads to where the evidence could be residing.

In our experience, companies can benefit by leveraging business intelligence across some key processes such as vendor or counterparty onboarding and management, investment due diligence, recruitment of C-Suite and other senior candidates, asset tracing, driving compliance programs focused on safeguarding labor laws and ensuring appropriate working conditions, and monitoring compliance of environmental, health and safety issues.

Response to fraud remains conservative

Survey respondents indicated that upon the detection of fraud, the top three actions taken by their organizations were internal investigation, disciplinary action against the fraudster, and renewal/ update of existing controls.

Internal investigations, though perceived as cost effective and confidential, have their limitations.

In our experience, internal investigators can be limited by their knowledge of investigative tools. It is also possible that their personal biases may influence the nature of the investigation. Additionally, internal investigators may also be challenged in the area of evidence handling and may unwittingly end up tampering with the legal admissibility of the evidence.

With regard to the action taken on the fraudster, we have seen that most companies tend not to terminate

the said employee, but pressurize him or her to resign from his or her duties. Further, there is little or no communication about the fraud to employees, as indicated by majority of the survey respondents.

In our view, while the sensitivity associated with certain frauds do not allow disclosure, communication of employee perpetrated frauds and the action taken by the organization against the perpetrators, gives employees a sense of the organization’s low tolerance for misconduct.

Survey findings also reveal that only a quarter of the survey respondents took legal action against the fraudster. We feel this is likely due to the long drawn out nature of legal proceedings in India with little sign of a conclusive verdict, as well as the quality of evidence available with companies.

Figure 10: What action is generally taken in your organization upon the detection of fraud?



Despite heightened awareness of fraud today, it appears that the attitude towards fraud continues to remain primarily reactive. However, with the Companies Act 2013 specifically addressing fraud and attaching responsibilities on various stakeholders such as the Board, Audit Committee, Independent Directors and Auditors for different aspects of fraud preparedness and response mechanisms, we are hopeful that a significant

number of companies will, in the years to come, be able to put in place robust processes that enable them to mitigate the risk of fraud, detect any suspected breaches in time, and respond effectively to identified misconduct. We believe that the Companies Act 2013 can be instrumental in changing corporate India’s mindset of looking at compliance as an investment and not a cost.

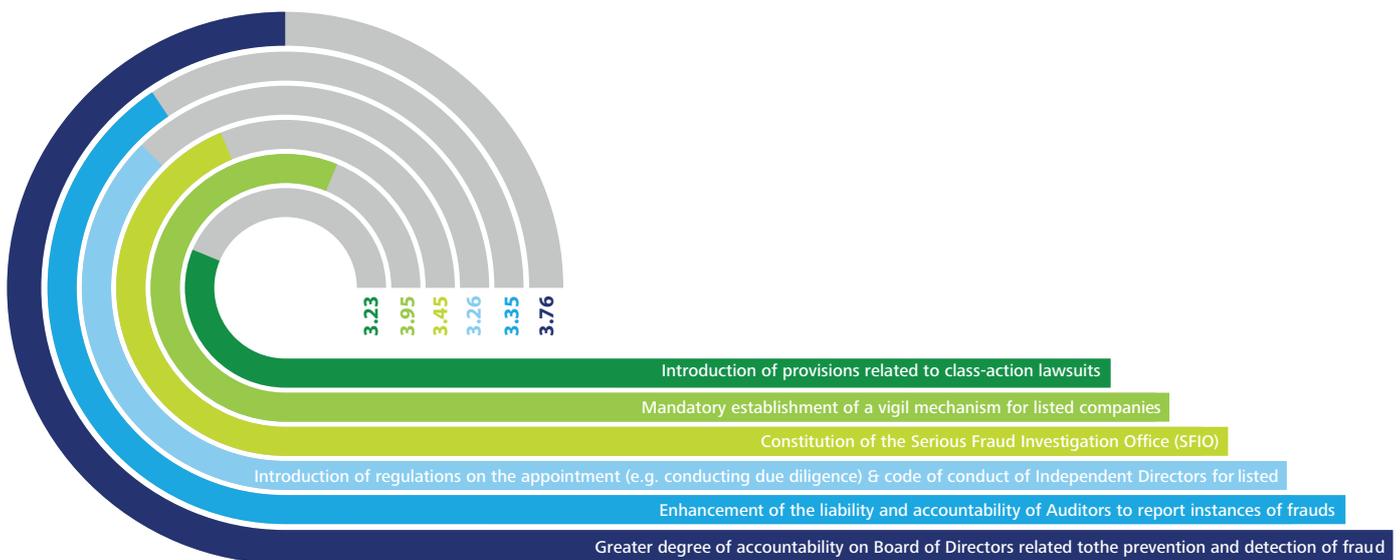
Impact of the Companies Act 2013 on the state of fraud

Comprehensive legislation combined with strong enforcement can be a big deterrent to fraud. The majority of the survey respondents agreed that the potential for enforcement and prosecution is a strong deterrent against fraudulent conduct. In this context, India's position on legislations to curb corporate fraud is still evolving.

The Companies Act 2013 is a significant development in the evolution of India's regulatory environment. This

law is the first in the country to focus comprehensively on fraud risk management and prescribes stringent punishment upon the violation of its provisions. The Act includes specific provisions to address the risk of fraud, alongside prescribing greater responsibility and increased accountability for independent directors and auditors. It goes beyond professional liability for fraud and extends to personal liability, prescribing penalties for directors, key management personnel, auditors and employees.

Figure 11: Which provisions under the Companies Act, 2013 do you think will be the most effective in fighting fraud? (Responses were ranked uniquely from 1 to 6, with 1- being least effective and 6 being most effective. Weighted average of scores is depicted below)



Effective enforcement of this legislation can reduce fraud significantly, according to 88 percent of the survey respondents. Among the provisions in the Act, survey respondents identified the mandatory establishment

of a vigil mechanism for listed companies, and a greater degree of accountability placed on the Board of Directors, as the most effective provisions in tackling wrongdoing

There has to be a dedicated unit in the organisation dealing with fraud risk management

– An independent director

Fraud risk management should be a compulsory item on the Board agenda and must be reviewed by the statutory auditors before they sign off the accounts.

– A survey respondent

Mandatory vigil mechanism

The Companies Act 2013 calls for the establishment of a vigil mechanism for directors and employees to report concerns about unethical behavior, suspected fraud or violations of the company’s code of conduct or ethics policy. However, the effectiveness of a vigil mechanism is not guaranteed by its mere existence, but by the confidence that stakeholders place in its functioning. As per the Deloitte India’s Whistleblowing Survey 2014⁵, survey respondents felt that a whistleblower program, should necessarily have the following key characteristics.

- a) Anonymity and confidentiality
- b) Adequate whistleblower protection
- c) Transparency and Independence, as required by the legislation, and to provide for an objective view
- d) A dedicated team to handle whistleblower complaints (third party or internal)
- e) A well-documented process of addressing complaints, feedback and communication.

Figure 12: What characteristics do you feel, a whistleblower hotline/ policy should have? Source: Deloitte India Whistleblowing Survey 2014



⁵ Source: Deloitte Forensic report titled: Lead by Example – Making whistleblower programs successful in corporate India - <http://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-fa-whistleblowing-survey-2014-noexp.pdf>

From an operational standpoint, a robust whistleblowing mechanism should feature multi-channel accessibility and multi-lingual support. Close to 38 percent of respondents to Deloitte India’s Whistleblowing Survey 2014⁶ identified the need for multiple reporting methods, such as a dedicated phone number, an exclusive email address or website, and the ability to receive complaints by post or fax.

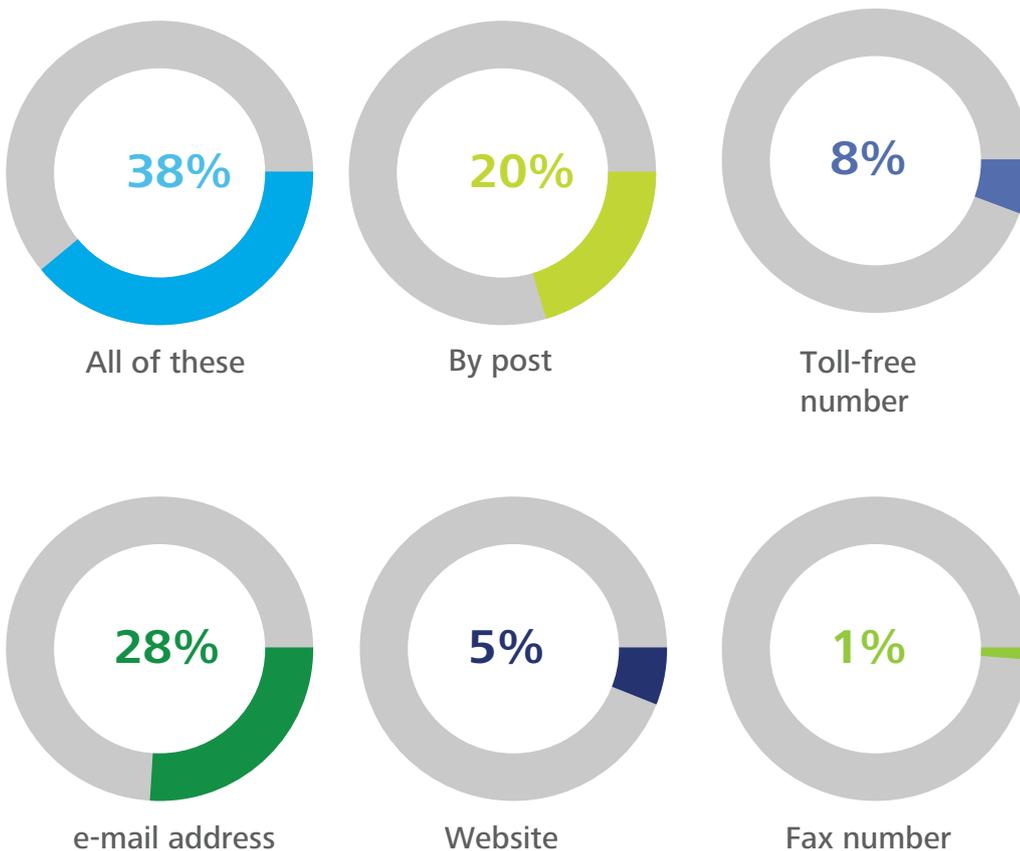
A comprehensive solution would be to engage a 24-hour response center staffed by multi-lingual officers to receive information, as well as analysts to prepare incident reports from disclosures received through any of these channels. Whistleblower reports are sensitive and not being able to use one’s preferred language can adversely impact a report’s completeness and accuracy. For many companies, whose operations span national

and linguistic borders, the ability to take reports in many different languages is absolutely essential.

Lastly, support from senior management is crucial to making whistleblower programs successful. For instance, senior officers at a company known to us, sent an email to all employees, sharing their experience of testing the whistleblower hotline, helping reassure their staff about how easy and confidential the whole process was. Subsequently, the company saw higher number of employees use the hotline.

Given the limited success that Indian companies have had in the past with their whistleblower programs, we would recommend a well-planned campaign to create awareness about the whistleblower program and its features to all stakeholders.

Figure 13: Which modes of access/ communication channels are crucial for an effective whistleblowing hotline? Source: Deloitte India Whistleblowing Survey 2014



⁶ Source: Deloitte Forensic report titled: Lead by Example – Making whistleblower programs successful in corporate India - <http://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-fa-whistleblowing-survey-2014-noexp.pdf>

Greater accountability on board and directors to prevent and detect fraud

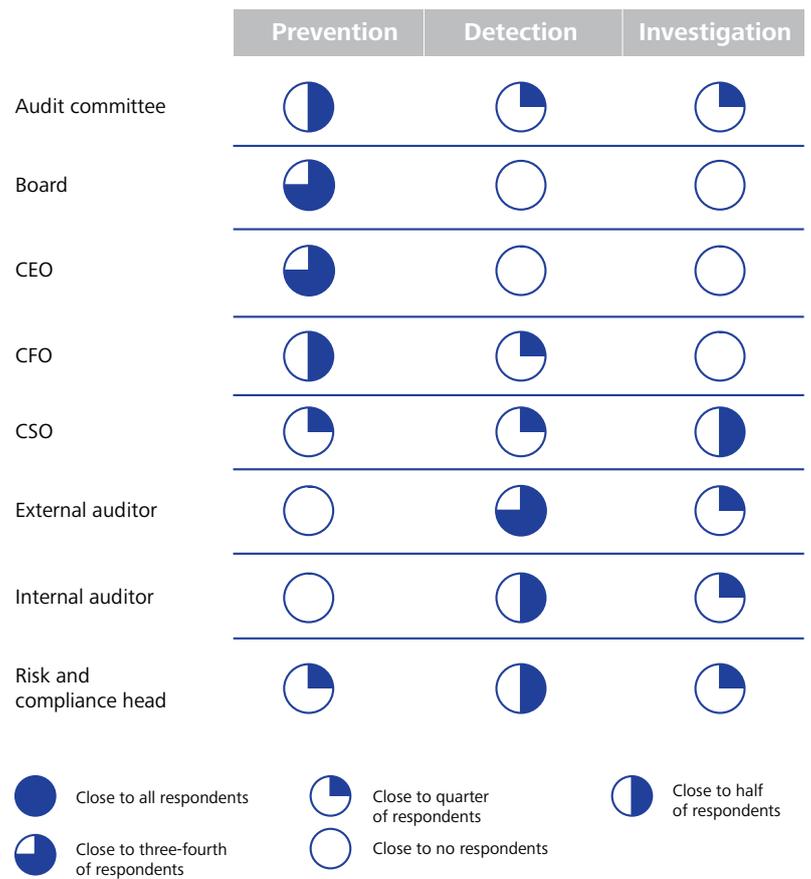
The majority of our survey respondents felt that the Board should be responsible for preventing fraud, while external auditors should be responsible for fraud detection. They also felt that the Chief Security Officer should be responsible for fraud investigation. In our view, it is not prudent to restrict these responsibilities to one individual/ team. Equal representation from the board of directors, audit committee and risk and compliance teams, can effectively utilize synergies to create a robust mechanism to monitor fraud incidents. Global research⁷ indicates that fraud risk management should not be restricted to be the role of a few Board members; in fact it has to be a combination of varied experts such as Internal Audit, Audit Committee, Information Technology, Ethics office, Security and staff.

Survey respondents have indicated that Internal Auditors should not be responsible for fraud prevention. In our view, the internal audit team is most familiar with the company’s processes and can therefore prove to be useful in preventing fraud.

Survey respondents also indicated that the Board’s responsibility should be restricted to fraud prevention. We, however, feel that the Board should take the onus of proactively monitoring their companies’ efforts to understand and mitigate fraud risks and also be involved in setting up a system through which investigations are performed and resolved competently and objectively, particularly in cases where the senior management may be involved in fraud. Further, active monitoring and Board oversight act as strong deterrents to fraud and enhance the perception of detection. These actions also demonstrate the ‘Tone at the Top’ and help set the platform for an internal antifraud culture.

Most of the survey respondents felt that external auditors should be held accountable for fraud detection. However, globally, over the last five years, external auditors have detected less than 5 percent of frauds within organizations and their contribution to fraud detection is steadily falling, with only 3 percent of frauds being detected by them in 2014⁸. In our experience, the inherent limitations of statutory audit, make it difficult for external auditors to detect fraud and therefore placing significant onus of fraud detection on them may not be adequate.

Figure 14: According to you, who should be responsible for the prevention, detection and investigation of fraud?



There is need for transparency especially on the appointment and functioning of independent directors
 – A survey respondent

⁷ Source: Whitepaper titled Managing Business Risk of Fraud, by Association of Certified Fraud Examiner - ACFE (US) - http://www.acfe.com/uploadedfiles/acfe_website/content/documents/managing-business-risk.pdf

⁸ Source: ACFE Report to the Nations on Occupational Fraud and Abuse - <http://www.acfe.com/rtrn/docs/2014-report-to-nations.pdf>

We are also seeing traction among companies making efforts to ensure that the senior management is equipped to deal with fraud. Survey respondents highlighted the key areas of focus as creating a zero tolerance culture, periodic communication to employees on ethical behavior, and review of code of conduct to include specific policies on fraud.

Alongside the efforts being taken to revisit the code of conduct and other documentation to extend the scope to cover fraud risks, it is also important to sensitize senior management to the risk of fraud because they are responsible for setting the tone at the top and cascading the message of fraud risk management to employees.

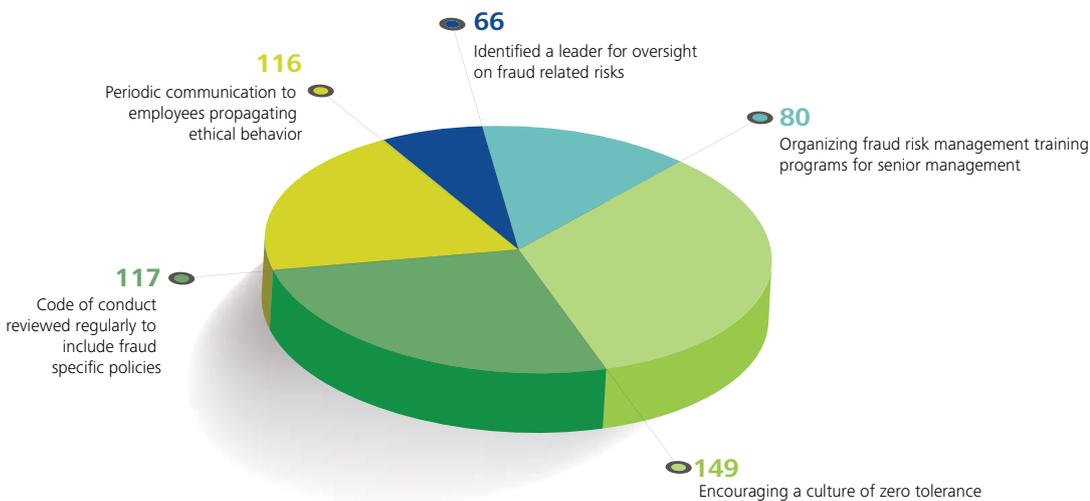
However, only 38 percent of survey respondents indicated that they organized periodic training programs for senior management on fraud risk management. In our view, the senior management team should spend time understanding the provisions under the Companies Act 2013, as several provisions indicate the need for a proactive approach to fraud risk management, as opposed to the existing reactive approach that survey responses have indicated throughout the survey. Complying with the provisions of the Act is possible only if the senior

management can recognize the gaps in compliance levels and take appropriate measures to plug them. Further, the Act prescribes penalties on the senior management (including up to 10 years of imprisonment and/ or fines of up to INR 25 Lakh) in case of fraud or noncompliance, making them personally liable for negligence.

To ensure compliance with the Companies Act 2013, we have observed that a few companies have identified 'fraud risk management champions' to drive the implementation of training programs across the organization. These leaders also served as a single point of contact to deal with all issues arising due to fraud, misconduct and noncompliance.

The Companies Act 2013, in our view, has challenged the fraud risk management efforts undertaken by companies in the past. Companies need to think strategically and make long term investments in tackling fraud. Setting up a dedicated internal investigations and response team, investing in data analytics tools to detect red flags, and including due diligence processes as part of the larger fraud risk management framework, are some initiatives that can prove to be helpful in the long term.

Figure 15: In line with the recommendations made in the Companies Act, 2013 what is being done at your organization to ensure that the senior management to deal with various complex fraud scenarios? (This is a multiple response question, statistics will not add upto 100%)



Section 2

Managing the face of fraud tomorrow



News frauds call for new armory

The world is seeing a rise in new frauds⁹ which the business community appears to be largely unaware of. Some of the key frauds uncovered in very recent times in the world are mentioned below.

The Deloitte India Fraud Survey has identified four emerging frauds that can significantly impact the way Indian businesses use digital media. These include social media fraud, e-commerce fraud, cloud computing fraud and virtual currency/ crypto-currency related fraud. Each of these frauds has been discussed in the coming pages, along with potential measures for mitigation.

Work from home scam
Photo sharing fraud
Encryption fraud
Spear-phishing
Research fraud
Collection scam Wi-Fi fraud
Voter fraud **Mystery shopper scam**
Holiday shopping scam
Ransomware fraud
Disaster relief fraud

⁹ Source: <http://www.fbi.gov/scams-safety/e-scams>

E-commerce fraud

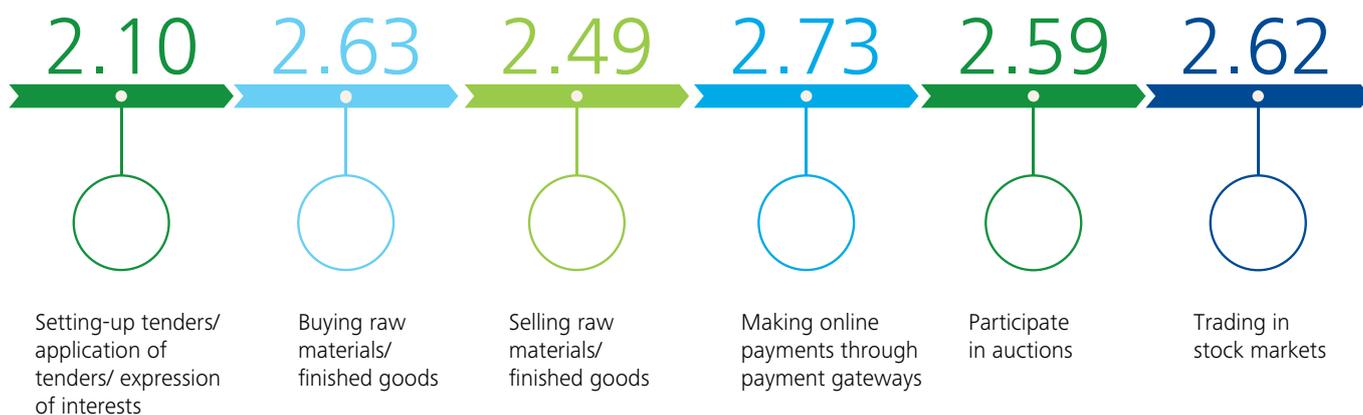
Electronic Commerce (E-commerce) encompasses all businesses conducted by the use of computer networks. The Indian e-commerce industry is currently valued at approximately INR 224 billion and is growing at the rate of 50-55 percent annually. It is expected to be approximately INR 504 billion large in the next two years¹⁰. Currently travel related bookings such as flight ticket, rail ticket and hotel bookings form the largest chunk of the e-commerce industry followed by online retail of consumer goods.

The primary reason for the growth of the e-commerce industry has been the increasing internet penetration in India. In 2006 there were only 21 million active internet users, whereas in June 2014, there were close to 243 million users¹¹. This rise in the number of

people familiar with, and able to access the internet, has spurred the development of online marketplaces. Almost three-fourths of our survey respondents said they were comfortable doing business online, although they considered some aspects of e-commerce transactions prone to the risk of fraud.

Online payments, procurement of materials, and trading in stock markets were identified as areas vulnerable to fraud risks. This is in line with global research which indicates that e-commerce payment fraud is on a rise. US-based research data shows that the value of fraudulent transactions is often four times the value of a regular transaction¹².

Figure 16: In your opinion how risky is it to conduct the following processes via online platforms? (Responses were rated from 1-5 with 1 – being least risky and 5- being most risky. Weighted average of scores is depicted below)



¹⁰ Source: The Hindustan Times news report - <http://www.hindustantimes.com/business-news/online-convenience-click-shopping-gains-consumers/article1-1190072.aspx>

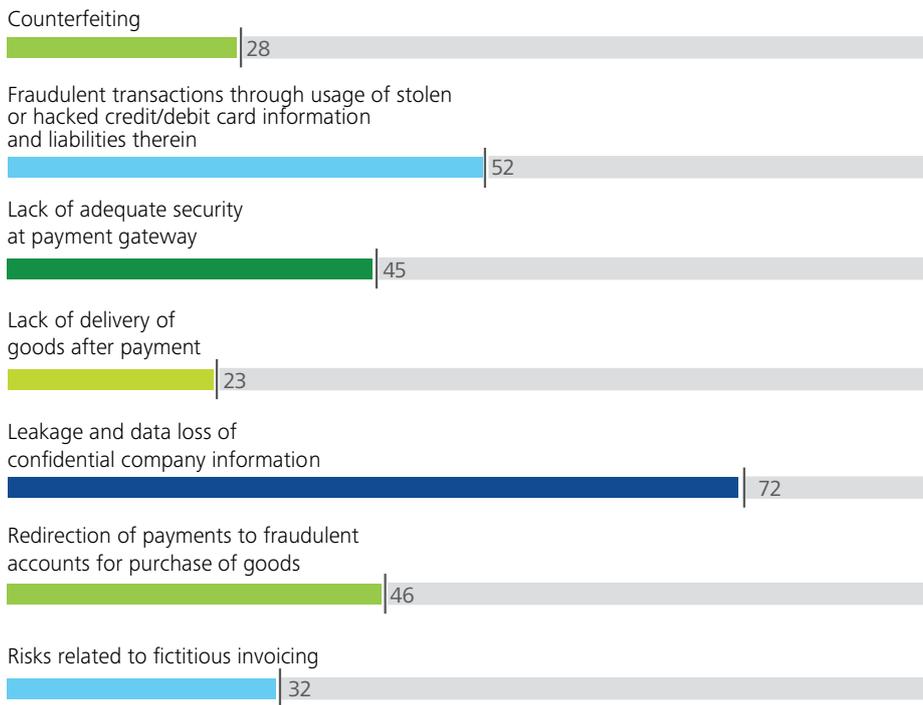
¹¹ Internet and Mobile Association of India, Press release - http://www.iamai.in/PRelease_detail.aspx?nid=3222&NMonth=11&NYear=2013

¹² Source: EMC- RSA Research - <http://www.emc.com/collateral/fraud-report/rso-online-fraud-report-0714.pdf>

Further, procurement of materials online is likely to be considered risky in India, due to concerns over the performance, availability and security of the materials purchased¹³. Further, many a times, sellers may not disclose data pertaining to the product, its quality, legality of use, and warranty. Each merchant can follow different standards for representing product related data, making it challenging for buyers to estimate the quality and legitimacy of products on sale. Traditionally, this risk was mitigated to some extent due to physical inspection of goods prior to purchase, and a predominant credit based business model that facilitated return of goods, if found unsatisfactory.

While the above mentioned fraud risks may not deter organizations from e-commerce trade, survey respondents mentioned other fraud risks, such as leakage and loss of confidential data, fraudulent transactions and inadequate security at payment gateways, that could deter their organizations from doing business online. This opinion can be attributed to global media coverage of such issues that highlight the difficulty in tracing the extent of data and fraud loss.

Figure 17: In your opinion, what are the key fraud risks that deter your organization from doing business online?



Some of the other prevalent e-commerce related frauds impacting buyers as well as merchants that may deter e-commerce transactions include the following:

1. **Site Replicating:** The fraudster replicates the original website with an aim to gather personal information from customers to defraud them. Information such as credit card details, bank account passwords and other personal details are unknowingly shared by gullible customers, and the fraudster uses this information to his benefit.

2. **Credit card chargeback:** Chargeback refers to a scenario when a customer disputes the amount charged on his/her credit card and refuses to honor the payment. This can occur in case of identity theft, when a customer claims that they did not authorize/ is unaware of the purchase charged on their credit card. The customer's bank then refuses to process the transaction and the merchant's revenue is held-up until the dispute is resolved.

¹³ Source: Book titled E-commerce, an Indian perspective, second edition, by P.T. Joseph, Page 50 - HYPERLINK "http://books.google.co.in/books?id=wDfPA4BChdAC&pg=PA38&dq=E-commerce,+an+Indian+perspective,+second+edition,+by+P.T.Joseph,+Page+50&source=gbs_toc_r&cad=4" \l "v=onepage&q=E-commerce%2C%20an%20Indian%20perspective%2C%20second%20edition%2C%20by%20P.T.Joseph%2C%20Page%2050&f=false" http://books.google.co.in/books?id=wDfPA4BChdAC&pg=PA38&dq=E-commerce,+an+Indian+perspective,+second+edition,+by+P.T.Joseph,+Page+50&source=gbs_toc_r&cad=4#v=onepage&q=E-commerce%2C%20an%20Indian%20perspective%2C%20second%20edition%2C%20by%20P.T.Joseph%2C%20Page%2050&f=false

3. **Sale of spurious/counterfeit goods:** Fraudsters may sell fake/duplicate products at significantly cheap prices, causing loss of revenue to the original merchant/manufacturer. The customer is duped with an inferior product that does not perform adequately, and is unable to claim a replacement or press charges for damages.

Prevention is better than cure

While we don't see fraud risks deterring corporates from transacting online, it would still be advisable to take measures to mitigate fraud risks. Some of the measures that merchants and customers can adopt to have a safer e-commerce experience include:

1. **Establish anti-fraud policies and procedures:**

Every merchant must have a policy on sales, online payments, sales returns, shipping, customer details verification and a fraud manual that identifies potential fraud risks. Buyer organizations can have a similar policy that details how to identify genuine e-commerce websites and guidelines on conducting business online. A section that helps identify and report fraudulent sites must also be included in the policies.

2. **Forming a dedicated team to monitor**

e-commerce frauds: Several companies have identified in-house teams that research on new frauds and communicate it to the organization. Such teams also challenge business processes regularly with an aim to unearth any gaps in controls. This proactive approach to identifying emerging frauds is an effective strategy, given the evolving nature of e-commerce business in India.

3. **Due diligence:** Given the large third party ecosystem that supports e-commerce in India, merchants need to ensure that they conduct adequate due diligence before associating with business partners. Further, this diligence can also be extended to check and verify genuine customers. Buyer organizations can also conduct due diligence on e-commerce service providers, as well as traders who use the platform, to ensure that they are transacting with reliable parties with a good reputation in the market.

4. **Communication and Training:** Communicating fraud risks and safeguards to employees and vendors can help prevent fraud incidents. Employees should be educated on safety mechanisms, identifying fraud risks, as well as conducting business ethically online, through periodic training programs.

The E-commerce model can help convert the largely unorganized retail sector to a technologically savvy organized sector. While India is in the process of developing a legislation which can be enforced on either the buyer or seller in terms of a framework within which business needs to be conducted, formation of contracts and the liabilities involved therein, nonetheless, cues can be taken from The United Nations Commission for International Trade Law (UNCITRAL), a model law on e-commerce which serves as a benchmark for national and international legislation and assists contracting parties in formulating their contracts. The UK's E-commerce regulation known as Electronic Commerce (EC Directive) Regulations 2002, clarifies and harmonizes the rules of online business throughout Europe with the aim of boosting consumer confidence.

While the government is working closely with e-commerce players and manufacturers to develop legislation that addresses the concerns of doing business online, companies should also aim to fortify themselves with adequate safeguards to mitigate the risk of fraud and reputation loss.

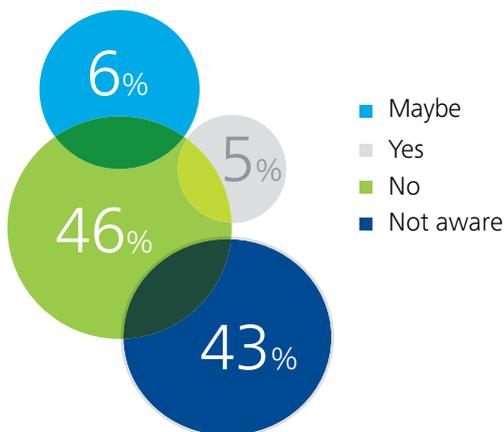
Cloud Computing fraud

With increasing number of users demanding simultaneous access to data and applications over multiple devices such as desktop PCs, notebook computers, smartphones and now smart watches, cloud computing is gaining appeal for both enterprise and personal use.

The current state of technology makes it possible to edit and share documents and data across multiple devices and locations. Some subscriptions also allow users to collaborate and interact in real-time.

As the number of cloud-based service providers grow, risk to systems and intellectual property have also grown. While well-known service providers have sophisticated security and access control systems, the safeguards employed by scores of lesser-known service providers may not be relatively well documented. Some of the key risks that users of cloud computing may face include, data loss from unauthorized use of low-quality systems, hacking, theft of intellectual property, and theft of confidential customer data.

Figure 18: Has your company experienced any issue due to cloud computing such as eavesdropping, account hacking/ hijacking, data loss and leakage etc.?



Fraud losses from cloud computing are difficult to estimate though the damage could be massive depending on the sensitivity of the data lost. It is therefore important that companies remain aware of the risks they can face while using cloud computing as part of their business operations.

It is not surprising that only 5 percent of survey respondents indicated that their organizations had sustained losses from cloud-based intrusions. Around 43 percent were unaware of data loss or leakages arising from hacking or hijacking of cloud services and a similar percentage of those surveyed reported no losses.

Mitigating cloud computing risks starts with defining a comprehensive policy. Such a policy should include the following key components –

- Prohibiting the use of cloud services that violate the company's data domicile policies¹⁴
- Screening, testing and deploying an enterprise-grade cloud solution that complies with the company's own security standards, reliability requirements and brand image
- Allocating end-to-end responsibility for audit and security management to a dedicated team
- Prescribing a usage policy for end-users that is consistent with the company's compliance policies, security procedures and code of conduct.

These components must be periodically reviewed and updated, in line with changes in the service providers' policies and feature upgrades.

This is where the bulk of Indian companies seem to have a challenge. Close to 58 percent of survey respondents were unaware of the frequency with which their compliance and security policies related to cloud computing were updated.

While survey respondents indicated that other preventive measures such as IT and software audits, signing non-disclosures agreements, and pre-engagement assurance via vendor due diligence are in use, there was no indication on periodic monitoring of fraud risk management measures. The majority of the survey respondents said IT audits were performed only at the time of vendor appointment and/ or yearly.

In our experience, conducting periodic IT audits or monitoring the data pertaining to cloud within organizations is not as cumbersome as it was in the early days of the Internet. By utilizing technology, one can monitor transactions in real time and use that information to conduct a meaningful audit.

¹⁴ Certain regulatory jurisdictions have specific rules around how and where data is stored. Some countries ban the storage of customer data on servers located or mirrored in another country.

Figure 19: How often are compliance and security policies pertaining to cloud computing reviewed in your organization?

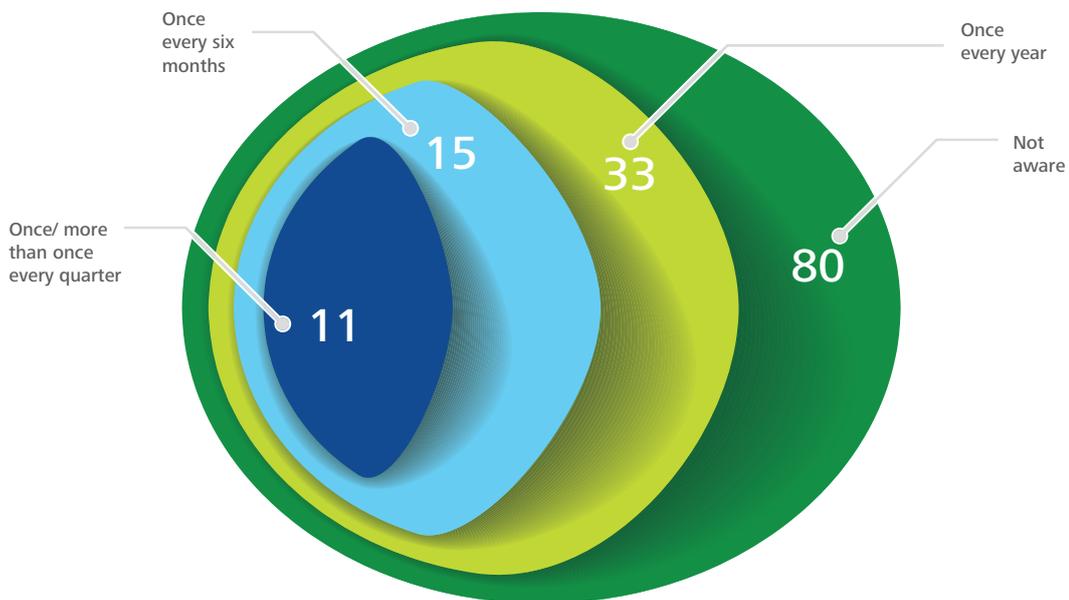
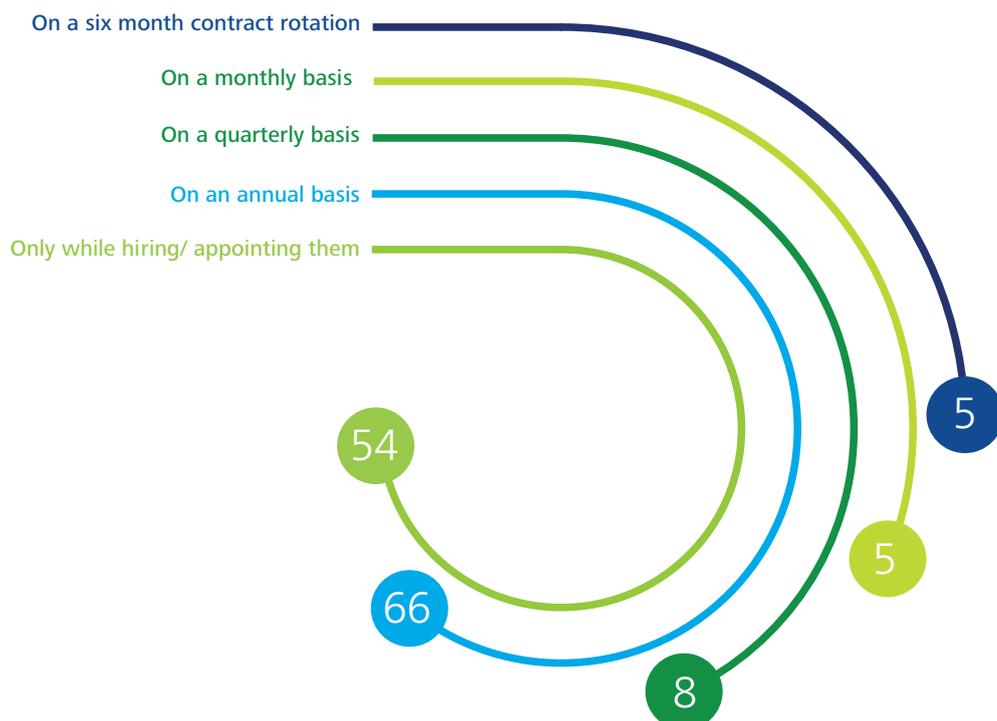


Figure 20: How often do you audit your third party IT vendor?



Social media fraud

Social networking is a valuable asset helping companies by providing strategic inputs, estimating competitive advantage and brand leverage, and also serving as a structured medium to buy and sell goods and receive feedback from users.

While companies have invested in establishing social networking platforms, it appears that few have a deep understanding of exactly how social media works, on the basis of the responses we have received for this section of the survey. As a result, social media remains an enigma for many executives, and most companies find it difficult to manage its operation and outreach, let alone the risks.

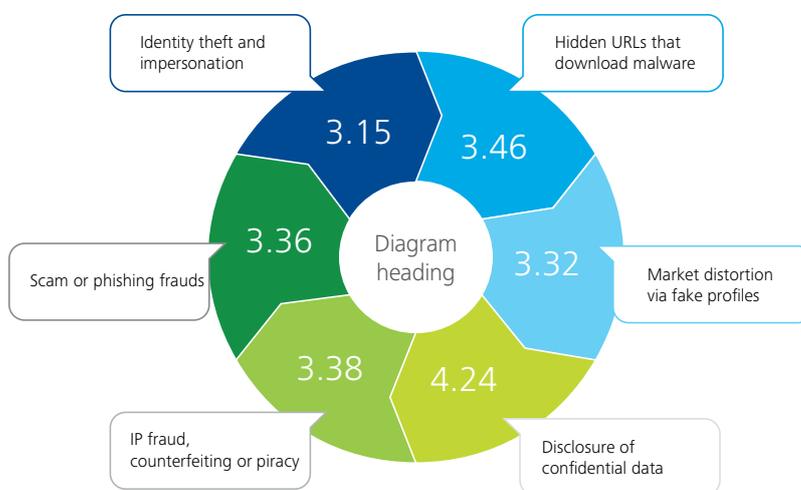
Our survey indicates that the most significant fraud risk concerning corporations is that of data disclosures. These include sharing of confidential information such as client names, financial details, reputation related matters, private employee related matters or forward looking information such as business plans. Recently, a leading cloud services provider came under scrutiny for the leak of several private pictures, some featuring high profile socialites or celebrities. It was later discovered that these pictures were shared by other users on popular social media platforms amplifying the damage to reputation. Due to the impact on reputation, there was considerable market share loss to most of the cloud providers.

The risk of data disclosure can be attributed to the lack of a formal training/ sensitization program for employees. Our survey respondents agree and over 61 percent indicated the absence of a formal policy or training on using social media in their organization.

Employees not educated in social-media matters pose the greatest risk when it comes to social business. Social-sphere activity may create situations not covered by traditional rules and risk frameworks. The use of social networks has, in an unprecedented way, blurred the line between employees' work and personal use of technology. As a result, the ways in which social platforms are used by employees give rise to a host of challenges for employers, including how best to protect confidential information.

Some of the common risks and corresponding mitigation measures that companies need to be aware of while using social media or allowing employees to use social media include:

Figure 21: According to you, which of the following frauds risks arising from social media could be the most damaging to your organization? (Responses were rated from 1-6 with 1 – being least damaging and 6- being most damaging. Weighted average of scores is depicted below)



- **Click-jacking** – Malicious hyperlinks are concealed beneath social media content that appears legitimate and upon clicking, the user ends up either downloading malware, or sending the user’s ID to a website, without his/ her knowledge. A variant of this type of fraud is cross-site scripting where malicious code is injected into a trusted website and upon access, infects the user’s system. A solution is to set browser options to maximize security and disable provisions of any scripting.
- **Doxing** – Fraudsters may hack into social media sites and publicly release personally identifiable information about individuals such as full name, date of birth, address, and private pictures. This information can be used to steal an individual’s identity and commit fraud, harass and bully individuals or coerce them into acting illegally or to extort money. To prevent instances of doxing, it is advisable to be careful of the information one shares about oneself, family, and friends on social media.
- **Scams** - Fake deals that trick people into providing money, information, or service in exchange for the deal. Cybercriminals use popular events and news

stories as bait for people to open infected email, visit infected websites, or donate money to bogus charities. It is recommended that people verify the validity of such deals by contacting the companies making the said offers on products.

Fraud and identity theft using social network sites as a tool is a fairly new and growing area of theft. A study found that 80 percent of users were concerned about privacy issues on social networking sites, yet almost 60 percent of them were unaware of what their own account's privacy settings were¹⁵. Considering there is little thought spent before sharing data on social networks, employees can endanger not just themselves but also their organizations, by accidentally sharing sensitive information.

Most social networking sites have a privacy setting in which a user can manage their own accounts. Altering the settings to make a user's profile totally private could be the difference between a user being safe or becoming an identity theft victim.

Approaches to mitigating social media fraud risks

Companies must strive to curtail compliance risks rather than deal with them at a time of crisis. A modus operandi for fraud gains traction in the absence of vigilance. Data privacy efforts and confidentiality clauses become remarkably efficient when coupled with clearly defined social networking protocols. Warning signs, security clearance and recurring trainings drive home the fact that the organization is actively under the scanner for the impending threats. This will ensure that companies can safely access social networking platforms to advance their business objectives.

We recommend that companies look at some of the below approaches to mitigating risks arising from social media.

- Develop clear policies on identifying and sharing confidential information on social networks. In our experience, many employers feel it is better to prohibit access to social media at work, to prevent instances of work-related communications taking place via social media.
- Ensure that the policy also details actions employees must do at the time they are leaving the company. In our experience, the tendency to share information

outside office networks is relatively high. Further, if an employee has been authorized to use social media as part of his role at the company, he/ she should be asked to limit their social interactions with third parties during the severance period to prevent any misuse of information.

- Encourage employees to disclose their use of social media during work times so that employer can devise a mechanism that is not too restrictive tempting employees to resort to other means to access social media. In many instances, we have seen companies allowing 30- 60 minutes access to specific social media networks via office systems to accommodate employee preferences, in return for an understanding that they will not misuse this privilege.

Inadequate legislative protection

About 68 percent of our survey respondents indicated that there was no adequate guidance in legislation to deal with social media fraud. For instance, the Indian law does not appear to be as comprehensive as the European General Data Protection Regulation¹⁶, which governs the storage, processing and movement of personal data (including personal data available on social media) within and outside the European Union. Further, the Indian government has indicated that Section 43A of the Information Technology Act has a comprehensive data protection provision, although there is no specific provision pertaining to social media. This appears to have created a perception among survey respondents that cases of social media fraud may not be dealt with any differently than other cases involving data theft.

Preventive measures

Organizations can consider deploying archiving software that enables the automatic capture and retention of social media content. Further, they can also implement data loss prevention (DLP) software to provide another layer of protection to prevent confidential and proprietary information from moving out of the company on to social networks. Employing a strong enterprise fraud and misuse management policy in parallel with upgrading one's network abilities to guard against threats can significantly improve the ability to mitigate potential risks.

¹⁵ Source: PC world article attributed to a research report by internet security firm Webroot http://www.pcworld.com/article/167511/beware_identity_thieves_social_networks.html

¹⁶ Source: Handbook on European data protection law, by the European Union Agency for Fundamental Rights, 2014 - http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

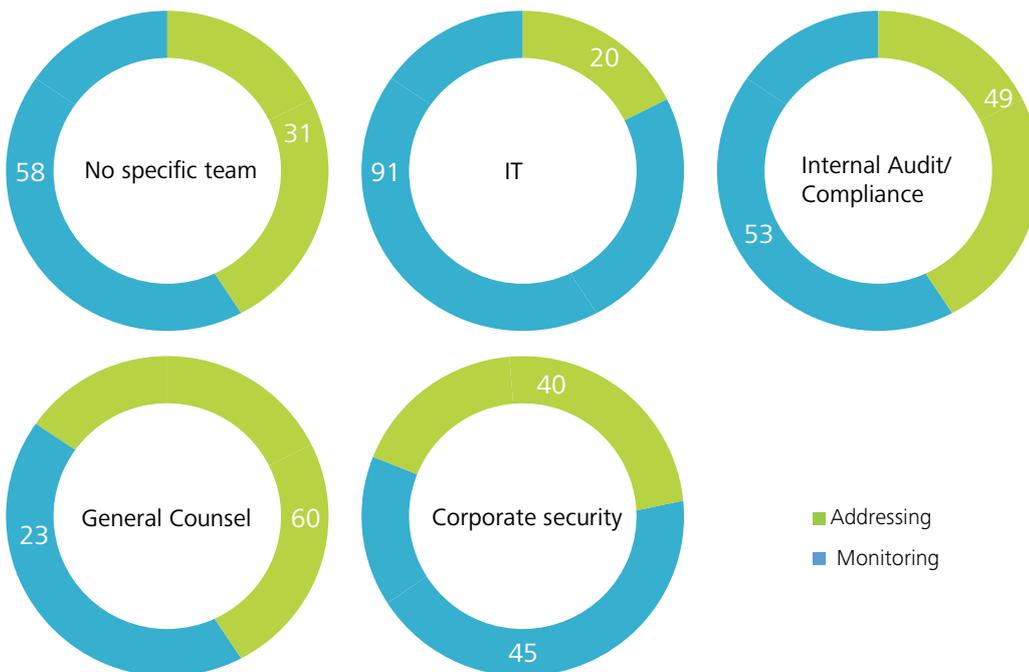
In this regard, entrusting the responsibility of fraud risk management to the right people can become key to the success of social media fraud prevention. Our survey respondents feel that the IT team should be responsible for monitoring fraud risks emanating from social media. In our experience, while the IT team can act as an effective enabler in the fraud risk monitoring process, they may not be the best suited to assess fraud risks. It is therefore advisable to have someone from the fraud control team / compliance team work closely with the members of the IT team, to better evaluate the risks arising from social media.

Over 50 percent of survey respondents also said that the General Counsel and Internal Audit committees should address any red flags that may arise indicating potential social media fraud. To better equip the General Counsel and the Internal Audit committee to address

these red flags, we feel that training and awareness about Information Technology laws would be helpful. Additionally, there are a number of social media monitoring software that many organizations use to track online reputation management. Exposure to such software can also help General Counsels and Internal Audit team members to understand the kind of red flags that may constitute social media fraud.

Social networks serve as extremely effective marketing tools and interpersonal mediums. The risk of publishing confidential information on social media platforms increases as organizations are increasingly sharing business related information on these to communicate with customers, partners and employees. Mitigating this risk is possible by developing a clear framework to evaluate risks, establishing a supporting infrastructure to take action, and a process to ensure that it operates successfully.

Figure 22: Who in your organization is responsible for monitoring and addressing frauds emanating from social media?



Virtual / Crypto-currency fraud

Virtual currencies exploded into public awareness in 2013, when a crypto-currency called Bitcoin was found to be a medium of exchange on a black-market website that was targeted by US law enforcement officials. For five years now, enthusiasts have mined this currency based on a complex computer algorithm and have been exchanging it for goods and services.

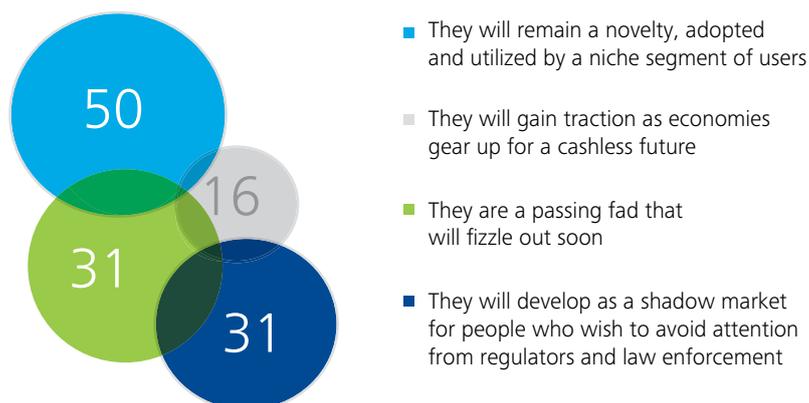
A virtual currency is an electronic unit to transfer value. These may range from mobile telecom credits that have evolved into a wider role, to sophisticated crypto-currencies like Bitcoin, Ripple or Litecoin. A crypto-currency is a medium of value transfer designed around securely exchanging information based on certain principles of cryptography. The most notable difference between a crypto-currency and existing monetary systems is that with the current state of technology, no group or individual may accelerate, stunt, abuse or in any way regulate the production of money beyond the principles upon which the system was built.

While most organizations may dismiss crypto-currencies as a passing fad, they seem likely to stay, given the number of businesses that support them. According to media reports¹⁷, a popular online retailer, a large computer manufacturer and a widely known internet-based travel services company, coffee shops and internet media providers are among the approximately 44,000 businesses and non-profit organizations across the world, which accept this crypto-currency. Various sources offer live exchange-rate tickers – one Bitcoin was worth USD 321 at the time of writing this report. A number of internet-based broking houses facilitate the exchange of traditional currencies for Bitcoins and the vice versa. All these could be signals that wider acceptance of crypto-currencies is imminent.

However, a majority of our survey respondents indicated that virtual currencies were not a part of their current strategy, with a large proportion predictably stating that they expect virtual currencies to remain a novelty – being adopted and utilized by a niche segment of users.

Even for its small user base, Bitcoin has proven to be vulnerable to widespread disruptions. Exchange rates have been volatile – reportedly due to speculative trading – and the industry has already experienced a round of bankruptcies affecting Bitcoin-dealing intermediaries. A large Asia-based Bitcoin broker collapsed amid reports of theft of Bitcoins worth close to half a billion dollars.

Figure 23: How do you see virtual currencies like Bitcoins developing in the long term?



These incidents prompt us to view crypto-currencies such as Bitcoin with a little more seriousness. A nearly untraceable medium of exchange, which can theoretically be used to store a billion dollars on a memory card of the type used in smartphones, is a massive concern for anybody tasked with preventing and detecting bribery, theft or fraud. Our survey respondents seemed to largely express this view indicating that the lack of oversight by regulators would expose market players to fraud risk.

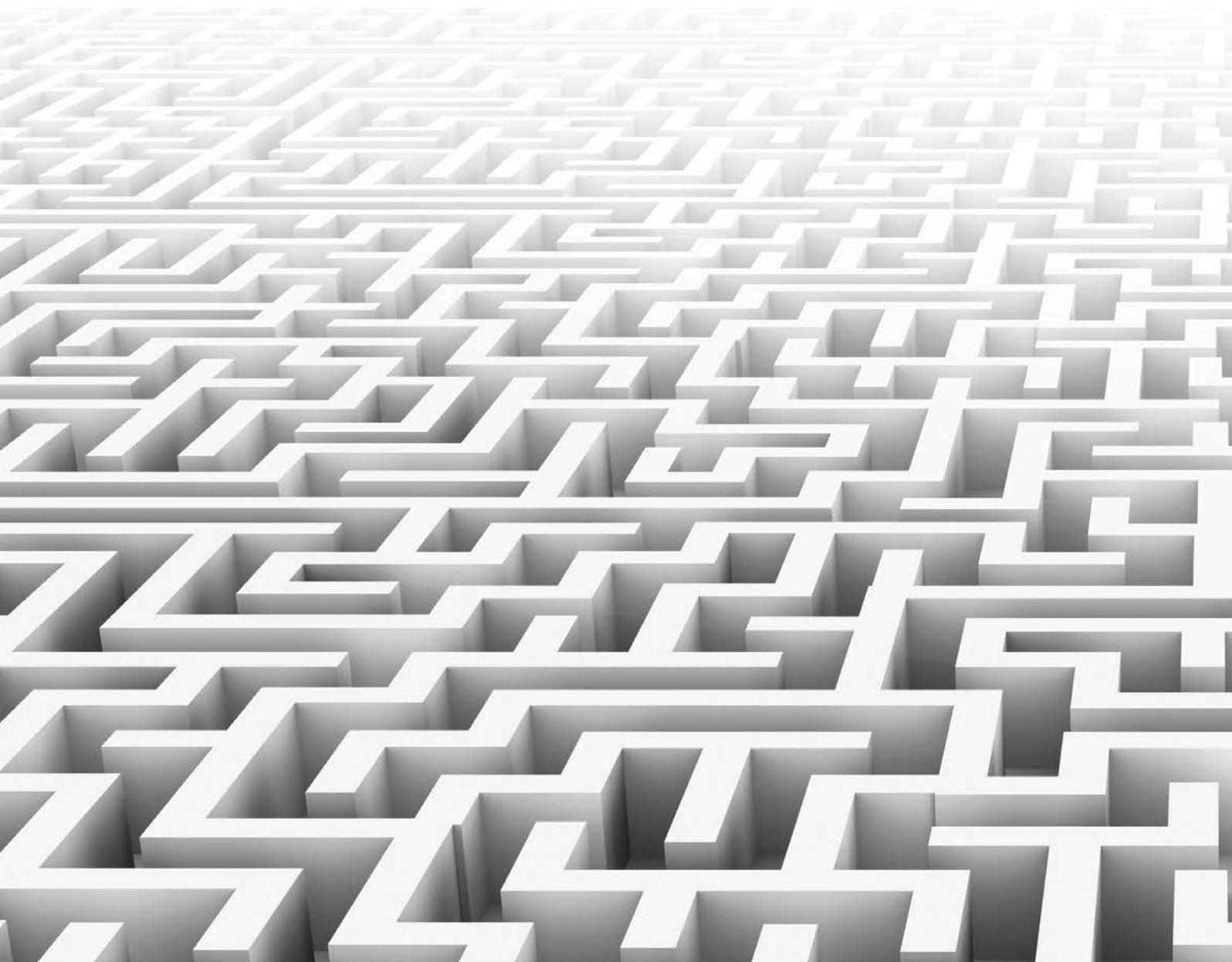
Regulators on their part have demonstrated mixed reactions on the emergence of virtual currencies. While some countries are yet to acknowledge the regulatory status of these currencies, authorities in many countries have warned consumers on the risks that they perceive. The UK Treasury has issued a 'Call for Information' on crypto-currencies; this is likely a precursor to a formal opinion or even a policy. Authorities in India have gone as far as warning the public that those engaging in virtual currency transactions may be in violation of the nation's Foreign Exchange regulations.

With the increasing interconnectivity of global asset markets, the past few years have seen unprecedented incidents of financial contagion. Will we ever see an incident where swings in Bitcoin or other virtual currencies will affect traditional financial markets? While an emphatic "no" is a tempting answer, it is too early to tell. For companies wanting to engage with these new currency models, a mix of robust risk management and judiciousness is the key.

¹⁷ Sources: <https://coldcrypto.com/shopping-paradise-using-bitcoin-online-store/>; <https://bitpay.com/directory/#/>; <http://pizzaforcoins.com/>; <http://www.sjearthquakes.com/news/2014/05/quakes-become-first-team-accept-bitcoin-payments>; <http://sanfrancisco.cbslocal.com/2014/01/16/larry-magid-sacramento-kings-to-be-first-professional-sports-team-to-accept-bitcoin/>

About the survey

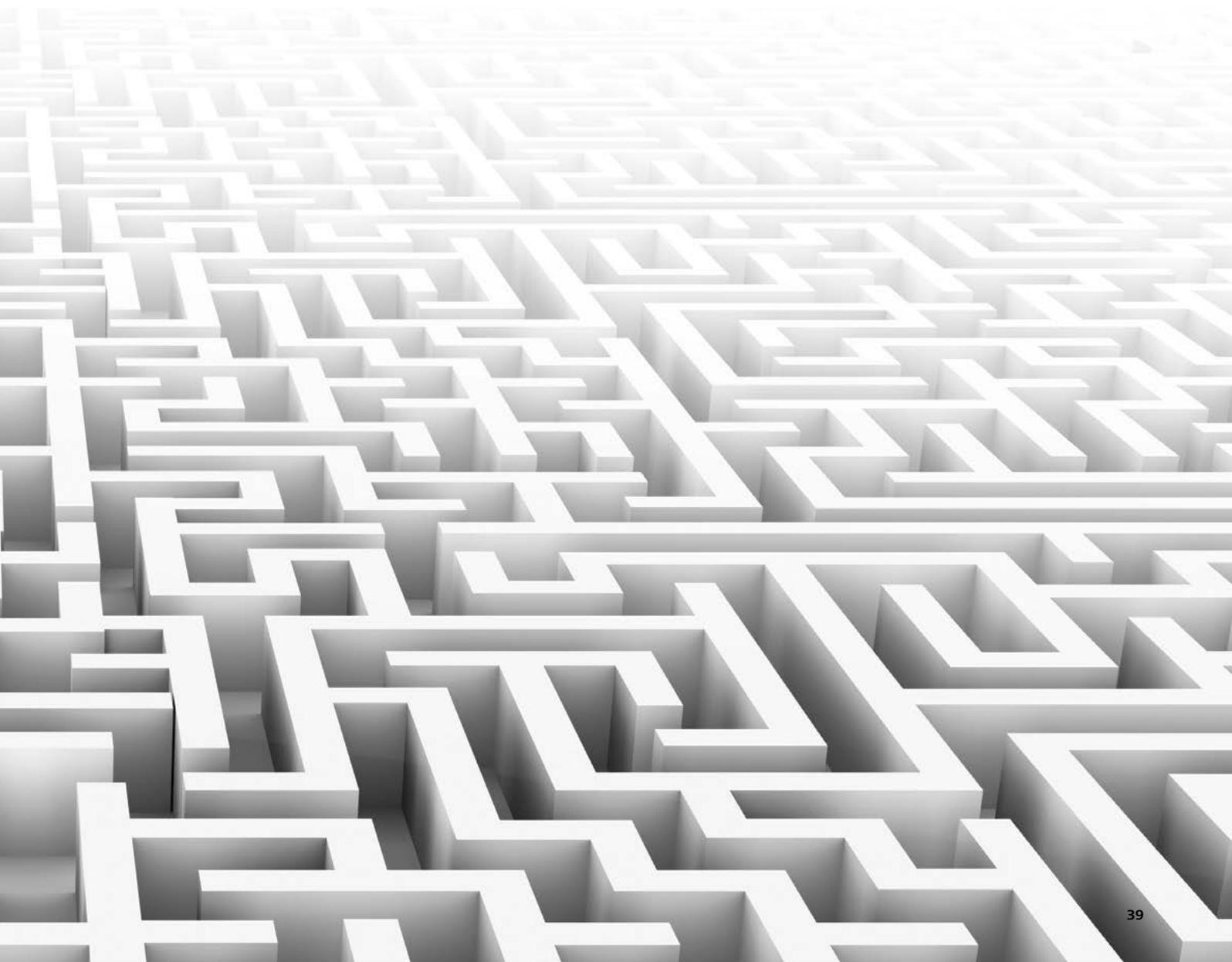
This survey report has been developed on the basis of responses received to a questionnaire that we circulated to leading CXOs across all major sectors working in the area of fraud risk management in September 2014. The response rate to questions varies and not all users have responded to all questions. In total, around 400 people responded to survey questions. Each statistic used in this report is derived from the number of responses to that question and must not be considered same across the report. For multiple choice questions, the weighted average of responses has been used to derive the statistic.



Acknowledgement

This survey report is the result of collective efforts from the following people in Deloitte India's Forensic practice: Adrija Sengupta, Ajit Nathaniel, Amrutha Yeshwanth, Anindita Singh, Archana Venkat, Dhruv Sengar, Kavita Nathaniel, Navaz Dubash, Pooja Meswani, Rajesh Chawla, Somyajit Sethi, Terence Sequeira, Vidhi Bang, and Vikram Savlani.

We would also like to thank the support extended to us by the IT, Brand and Risk teams at Deloitte India for helping us release this survey.



About Deloitte Forensic

Deloitte India's Forensic team helps companies identify and deal with a wide range of financial irregularities or fraud, misconduct and business disputes, and delivers clear, logical analysis, and fact finding reports. These outcomes are facilitated by a variety of quantitative and qualitative techniques to isolate and analyze information resulting from a number of circumstances.

We periodically release thought leadership documents that help shape the fraud risk management efforts undertaken by our clients and prospects.



Contacts

Rohit Mahajan

Head of Forensic

Tel: +91 22 6185 5180

Email: rmahajan@deloitte.com

Gordon Smith

COO and Senior Director

Financial advisory

Tel: +91 22 6185 6765

Email: gordonsmith@deloitte.com

Amit Bansal

Senior Director

Forensic

Tel: +91 22 6185 6764

Email: amitbansal@deloitte.com

Sumit Makhija

Senior Director

Forensic

Tel: +91 124 679 2016

Email: sumitmakhija@deloitte.com

Nikhil Bedi

Senior Director

Forensic

Tel: +91 22 6185 5130

Email: nikhilbedi@deloitte.com

KV Karthik

Senior Director

Forensic

Tel: +91 22 6185 5212

Email: kvkarthik@deloitte.com

Suprabhat NM

Director

Forensic

Tel: +91 22 6185 5214

E-mail: suprabhatnm@deloitte.com

Veena Sharma

Director

Forensic

Tel: +91 22 6185 5213

Email: vesharma@deloitte.com

Samir Paranjpe

Director

Forensic

Tel: +91 22 6185 5209

Email: sparanjpe@deloitte.com

Sushmit Bhattacharya

Director

Forensic

Tel: +91 22 6185 5263

Email: bsushmit@deloitte.com

Tanmay Bhargav

Director

Forensic

Phone: +91 (124) 679 2088

Email: tbhargav@deloitte.com

Sebastian Edassery

Director

Forensic

Tel: +91 80 6627 6157

E-mail: edasserys@deloitte.com

Nitin Bidikar

Director

Forensic

Phone: +91 (022) 6185 4829

Email: nbidikar@deloitte.com

Wifred Bradford

Director

Forensic

Phone: +91 (022) 6185 5505

Email: wbradford@deloitte.com

Rohit Goel

Director

Forensic

Phone: +91 (124) 679 2340

Email: rogoel@deloitte.com







Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material and the information contained herein prepared by Deloitte Touche Tohmatsu India Private Limited (DTIPL) is intended to provide general information on a particular subject or subjects and is not an exhaustive treatment of such subject(s). This material contains information sourced from third party sites (external sites). DTIPL is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such external sites. None of DTIPL, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this survey, survey results or any other information, rendering professional advice or services. The survey, survey result or any other information herein is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this material.

©2014 Deloitte Touche Tohmatsu India Private Limited. Member of Deloitte Touche Tohmatsu Limited