Deloitte.

India Fraud Survey
Edition II

Forensic ●

Foreword

Disruptive events, enabled by disruptive technologies and business models are increasingly characterizing both the Global and the Indian economy. The rapid pace of adoption of e-commerce, online banking, and social media means consumers today have access to information about products and services before they are formally introduced in the market, and are able to pass judgement on their effectiveness. Events such as the recent demonetization announcement by the government are further changing the dynamics of the economic environment. Regulatory frameworks, particularly those that govern business conduct, are evolving to keep pace with these developments.

In this dynamic environment, traditional businesses can no longer afford to sit back, unscathed by the changing world around them. Organizations have little choice but to adapt and remain relevant to customers. While some may see this as an unsurmountable challenge, fraught with uncertainty, I feel we are fortunate to witness the evolution of a new economic order.

India and Indian businesses, no doubt, will continue to grow in size despite the challenges they face. Businesses that succeed in becoming agile, leveraging technology effectively, and innovating consistently, will be more likely to emerge winners in this race for economic dominance. A lot of this success would also depend on how businesses structure themselves internally – such as having a strong focus on instituting robust internal processes and controls, reliance on automation for monitoring transactions and identifying suspicious activity, gathering business intelligence through analytics, and developing transparent governance models. Incidentally, these are among the areas that India organizations have traditionally been slow to develop.

The limited preparedness to foresee the impact of changing trends and build a robust backend supporting system can slow down progress and make organizations vulnerable to several risks including those of fraud. This edition reveals the inertia among large and small organizations in their fraud and noncompliance management efforts. It also provides suggestions that organizations will find useful in their quest to know and fight emerging fraud and noncompliance issues.

I hope you find this report a compelling read, as I did.

Regards
N Venkatram

Introduction

"Fraud is rising in India," "stopping fraud is the responsibility of the CEO," "fraud cannot be eliminated," and "junior people commit frauds." These are some of the sentiments on fraud we hear as part of our jobs. One topic, multiple perspectives.

Today everyone has an opinion on fraud. Be it a working professional, far from the rigors of the finance discipline or a small company struggling to recover losses, or a multinational concerned about reputation. It is this diversity of opinions and experiences that makes the fraud landscape in India complex. Consequently, fraud risk management efforts tend to become unique and challenging across organizations.

This is what our survey results also indicate. Multinational organizations appear to be primarily focused in preventing known frauds such as bribery and corruption, diversion/ theft of funds and vendor favoritism, even as the business landscape exposes them to new fraud and noncompliance risks such as cybercrime, social media and anti-competitive behavior. So while we observe increased adoption of automation and continuous monitoring as part of fraud risk management efforts, these initiatives will always find it challenging to detect new and emerging frauds.

Small and medium enterprises on the other hand, appear to be struggling to mitigate old menaces such as bribery and corruption, indicating a lack of commitment and resources to dedicate towards fraud risk management. Given the inherent limitations of these organizations, there is need for government intervention to help small and medium enterprises tackle fraud. In this regard, increased digitization in all spheres of business combined with strong enforcement of anti-fraud laws may benefit small organizations.

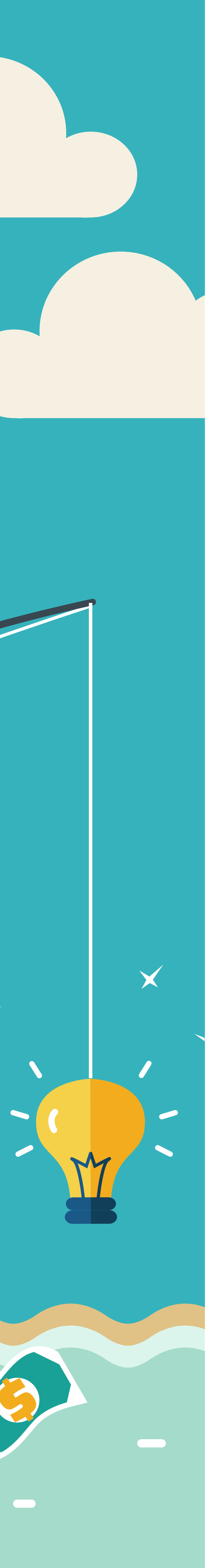
Successful fraud risk management efforts tend to go beyond strong internal controls or the presence of policies. Employees can play an influential role in the success of fraud risk management efforts, as indicated by a majority of respondents to our working professionals' fraud survey. Perhaps it is time organizations – large and small – nurtured a community of 'employee influencers' who can reinforce ethical behaviors and mitigate the risk of fraud.

The 2016 edition of the India Fraud survey also puts the spotlight on five new business trends that will likely impact the fraud landscape in the future –Blockchain, Internet of Things, Robotics, Cashless transactions and Online market places. As a first, we also have perspectives from the Deloitte member firms in Japan and Australia on the fraud concerns in their countries and possible challenges faced by some of their clients while working in India.

We hope you find this survey report useful.

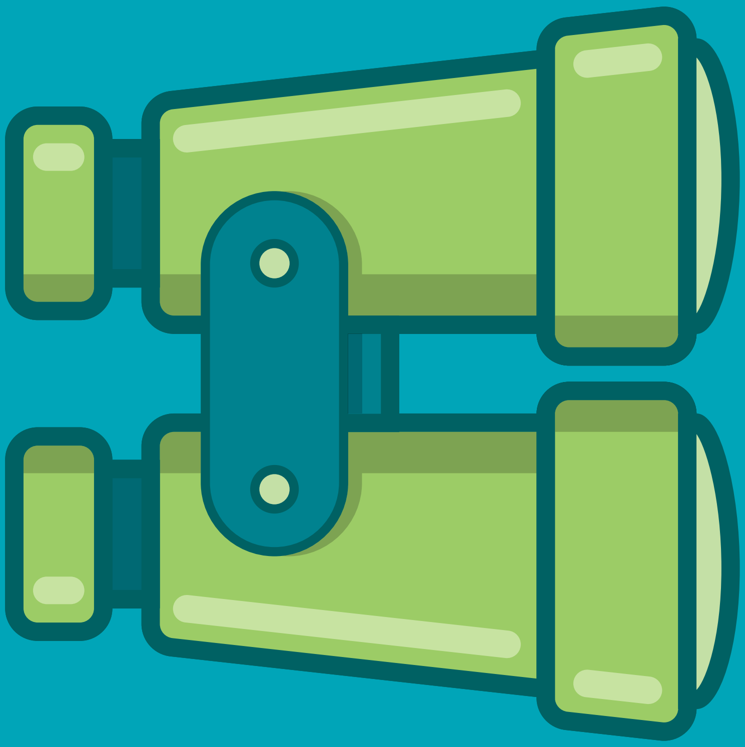
Uday Bhansali
President - Financial Advisory
Deloitte India

Rohit Mahajan
APAC Leader, Partner and Head – Forensic
Financial Advisory, Deloitte India



Contents

Key findings



Large companies' survey

- Perspectives from companies with over ₹ 200 Crore turn over and/or over 200 employees

70% of respondents felt incidents of fraud will increase in the next two years

Top reasons that contribute to fraud include – diminishing ethical values (38%), lack of efficient control system (37%), inadequate due diligence (37%) and unrealistic goals linked to monetary compensation (37%)

Vendor favoritism (42%), diversion/ theft of funds (33%) and bribery and corruption (30%) were the top fraud incidents experienced by organizations

Procurement (35%) and vendor/ partner selection (25%) were considered the functions most vulnerable to fraud risks

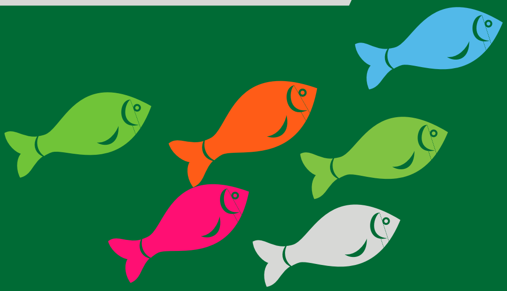
Junior and Middle management employees were considered the most likely to commit fraud

Top three measures undertaken to prevent fraud include – Internal Audit/ Risk assessment (89%), Tone at the top and implementation of anti-fraud policies (79%), and fraud awareness workshops and trainings (66%)

Fraud is mostly detected through whistleblower hotlines

Response to fraud is complex and determined on a case to case basis – 43% said investigations were commenced based on the severity of fraud; 36% said the fraudster was allowed to resign in lieu of pressing legal charges; and 33% said fraud was communicated to employees, the Board and regulatory agencies

Preparedness to emerging fraud and noncompliance risks such as social media and anti-competitive behavior appears to be low



Small and medium enterprises survey

- Perspective from companies with under ₹ 200 Crore turn over and/or under 200 employees

54% of respondents felt incidents of fraud will increase in the next two years

Top three reasons that contribute to fraud include the following – diminishing ethical values (68%), limited/ lack of segregation of duties (68%) and limited employee education on fraud (60%)

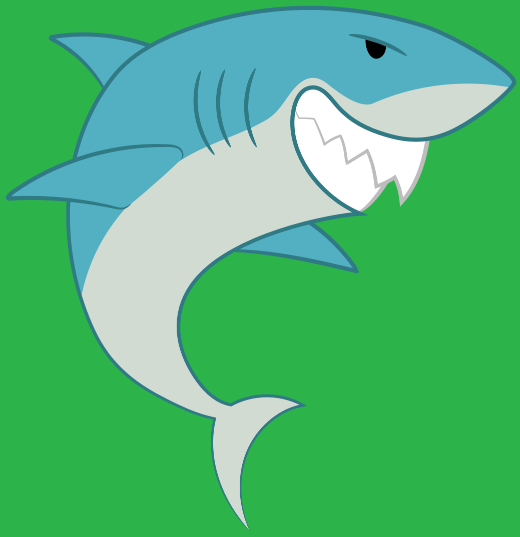
Top three frauds experienced by organizations include – Diversion/ theft of funds (32%), bribery and corruption (28%) and conflict of interest (26%)

The most common forms of corruption experienced include – collusive bribery (69%) and facilitation payments (69%)

Procurement (44%) and sales and distribution (29%) were considered the functions most vulnerable to fraud risks

32% felt complying with anti-fraud regulation placed additional burden on them

Fraud prevention efforts were found wanting – 48% felt there wasn't enough commitment; 42% felt there was inadequate budget and resource allocation to prevent fraud; 25% reviewed their fraud risk management frameworks only upon an incident occurring; and 23% addressed fraud observations within 1-2 months of the incident

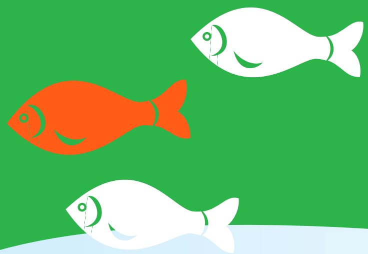


Top three measures undertaken to prevent fraud include – Independent Audits (71%), implementing a code of conduct (62%), and regular monitoring and assessment of fraud risks (52%)

Deploying technology to curb fraud is a challenge with 17% citing budgetary constraints, and 23% claimed lack of clarity around the utility of such tools

Response to fraud is complex and determined on the basis of the materiality of fraud (19%)

Top actions taken upon detection of fraud include – internal investigation (71%), review/ updating of existing controls (53%) and asking the fraudster to resign (53%)



Working professionals' survey

65% of respondents felt incidents of fraud will increase in the next two years

Top three reasons that contribute to fraud include – Weak/ ineffective controls (65%), technological advancements (43%), and general decline in ethical values (42%)

Top three frauds experienced by organizations include – bribery and corruption (43%), financial statement fraud (40%), and embezzlement of funds (39%)

Frauds personally experienced by working professionals include –bribery and corruption at government offices (59%), identity theft (37%) and sector specific frauds (31%)

In response to fraud, 55% of respondents claimed they did nothing as there was no way to recover losses

70% felt their employers encouraged them to provide enough opportunities to share instances of unethical behavior

Are laws on curbing fraud effective? – Yes (47%), No (42%)

Primary responsibility to fight fraud lies with the citizens (56%)

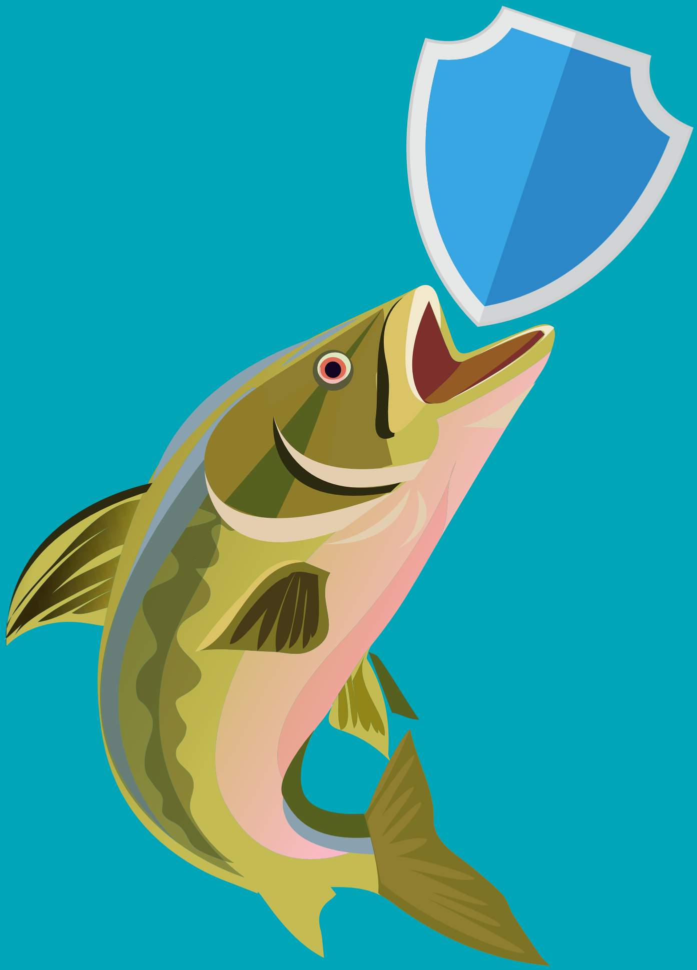
Top three measures the Government can take that will help reduce fraud in India – stronger enforcement (90%), greater adoption of technology (63%) and government advisory on key fraud schemes (63%)

Top 3 measures that corporates can take to reduce fraud – openly discuss fraud and educate employees (61%), recognize and reward ethical behavior (59%), and name and shame wrong do-ers (57%)

Focused on safeguarding themselves from well-known frauds, large companies grapple to understand emerging frauds

Conventional frauds continue to dominate the fraud landscape

In line with our 2014 survey, around 70% of Corporate India continues to believe that fraud will rise over the next two years. Fraud was attributed mainly to diminishing ethical values, lack of an effective/ efficient control system, inadequate due diligence on employees/ third parties and unrealistic targets/ goals linked to monetary compensation, indicating that fraud continues to be driven by concerns internal to the organization. Correspondingly, procurement (35%), vendor/ partner selection and management (25%), and sales and marketing (18%) were identified as the functions most susceptible to fraud. Among the type of frauds experienced, survey respondents indicated vendor/ customer/ business partner favoritism, diversion and bribery and corruption as the top three frauds. Further, the survey indicated that organizations could lose an average of between ₹10 Lakh and ₹1 crore to fraud. A little more than a quarter of respondents indicated they were unable to quantify the fraud loss.



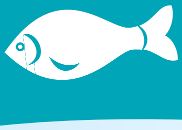
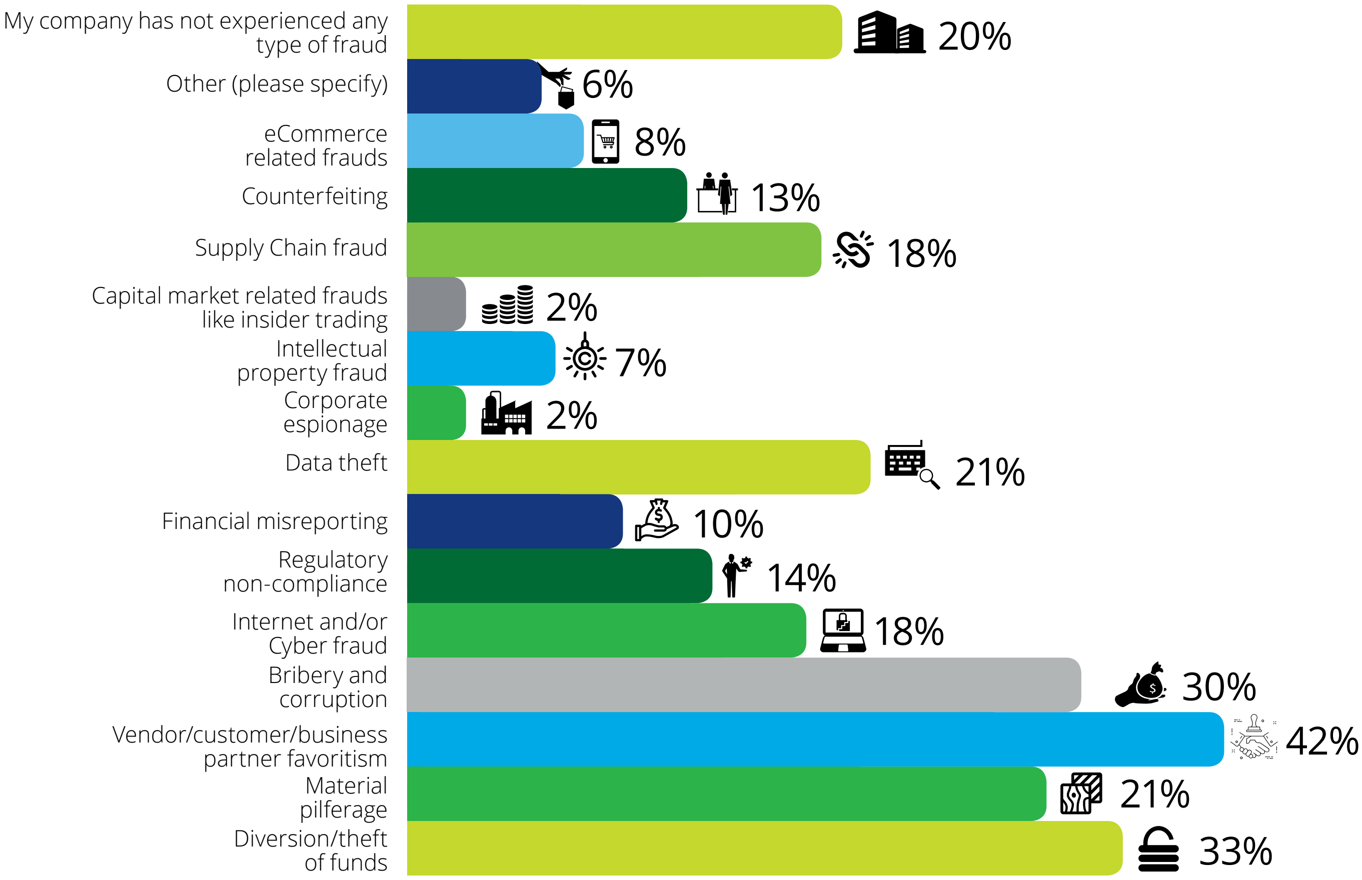


Figure 1: Which of the following types of fraud/misconduct/ malpractice has your organization experienced in the last two years?



Note: This is a multiple choice question and responses will not add up to 100%

Interestingly, while respondents did not rate bribery and corruption as the most common fraud experienced by their organizations, favoritism in appointing vendors and business partners is often in the backdrop of kickbacks and bribes being exchanged between colluding parties. It appears that organizations may be differentiating between private bribery and public bribery schemes: the former does not involve a government servant, but employees of private organizations colluding with each other for mutual benefits.

Given the robust anti-bribery and corruption compliance policies that large domestic and multinational corporations have in place, it is heartening to note that organizations may now be tackling public bribery better than they may have in the past. However, in our experience, private bribery schemes are no less dangerous to organizations.

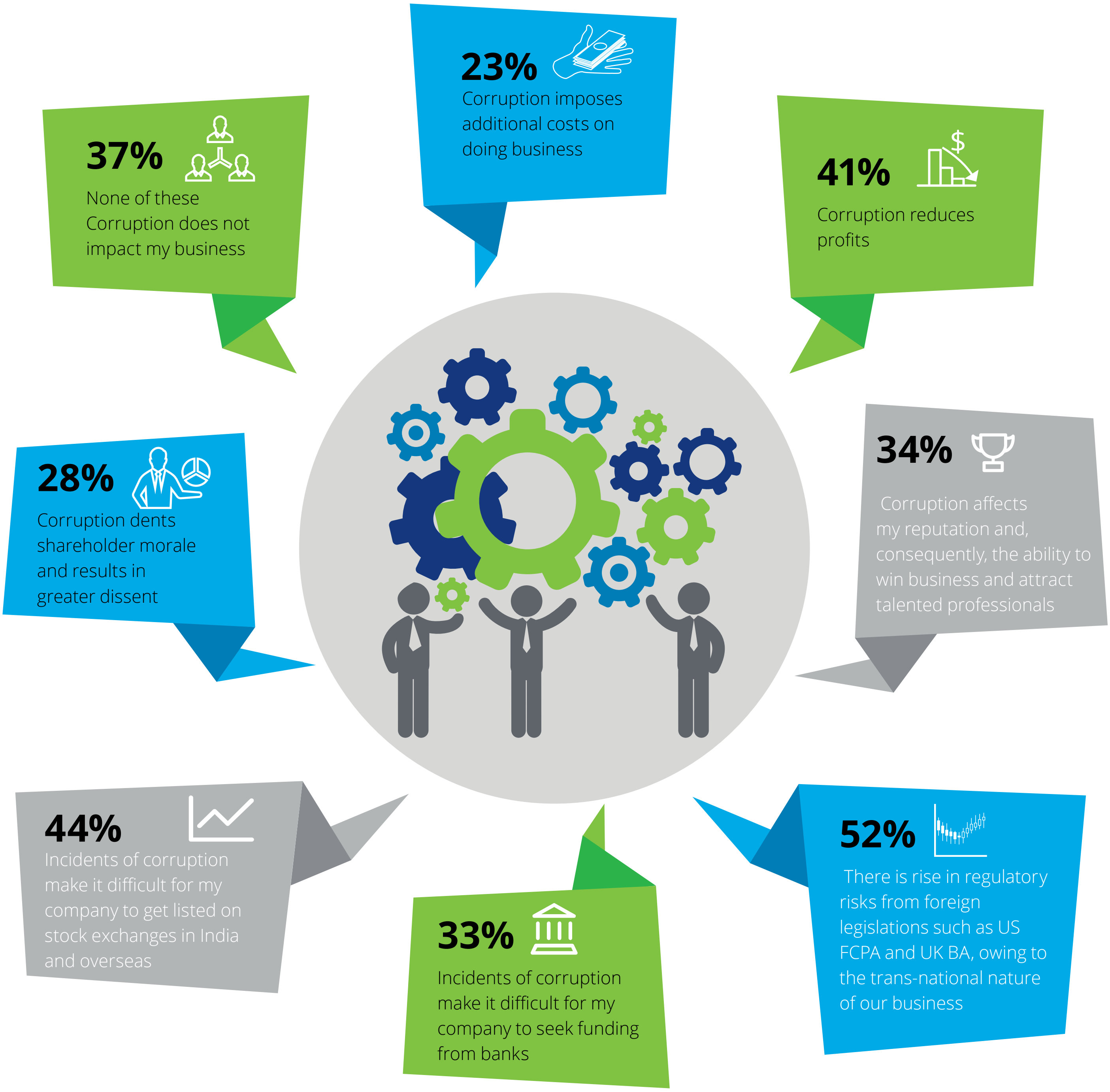
Potential conflict of interest, deteriorating product/ service quality as a result of hiring favored business partners, and diversion/ theft of funds are some of the possible outcomes of indulging in private bribery schemes. Upon unearthing of such schemes the organization in question may face reputational damage from the media, denial of capital from financial institutions and volatility in stock prices. Although currently there is requirement for a law that specifically prohibits private sector bribery[1], indulging in it may be a potential violation of the Companies Act, 2013 as well as Clause 49 of the SEBI Listing Agreement that seeks to reinforce good corporate governance and fraud risk management[2].

[1] The proposed amendments to the Prevention of Corruption (Amendment) Bill, 2013 cover organizations who indulge in bribe- giving, unlike the 1998 Act that only covered public servants who were recipients of bribery. Further, the draft Indian Penal Code (Amendments) Bill, 2011 is the only proposed legislation that encompasses graft / corruption by individuals, firm, society etc that undertakes any economic activity.

[2] The companies Act, 2013, looks at bribery and corruption as practices that may amount to fraud schemes such as procurement fraud, diversion of goods/theft etc. Although, the act of indulging in bribery itself is not a violation of the Act, the resulting fraud and the inability of organizations to prevent it may result in a violation. Similarly, if the end result of private bribery involves insider trading and unauthorized related party transactions, these actions may violate Clause 49 of the SEBI listing agreement. Source - http://www.mondaq.com/india/x/434208/Securities/Disclosures+Under+SEBI+Listing+And+Disclosure+Regulations+2015

In the area of public corruption, there appears to be increased awareness of how indulging in such practices can impact the organization. Overseas regulatory noncompliance (52%), potential difficulties in being enlisted on stock exchanges (in India and overseas) (44%) and reduction in profits (41%) were perceived to be the most damaging outcomes of indulging in bribery and corruption.

Figure 2: In your opinion, what are the ways in which corruption can impact your company?



37%
None of these Corruption does not impact my business

23%
Corruption imposes additional costs on doing business

41%
Corruption reduces profits

28%
Corruption dents shareholder morale and results in greater dissent

34%
Corruption affects my reputation and, consequently, the ability to win business and attract talented professionals

44%
Incidents of corruption make it difficult for my company to get listed on stock exchanges in India and overseas

33%
Incidents of corruption make it difficult for my company to seek funding from banks

52%
There is rise in regulatory risks from foreign legislations such as US FCPA and UK BA, owing to the trans-national nature of our business

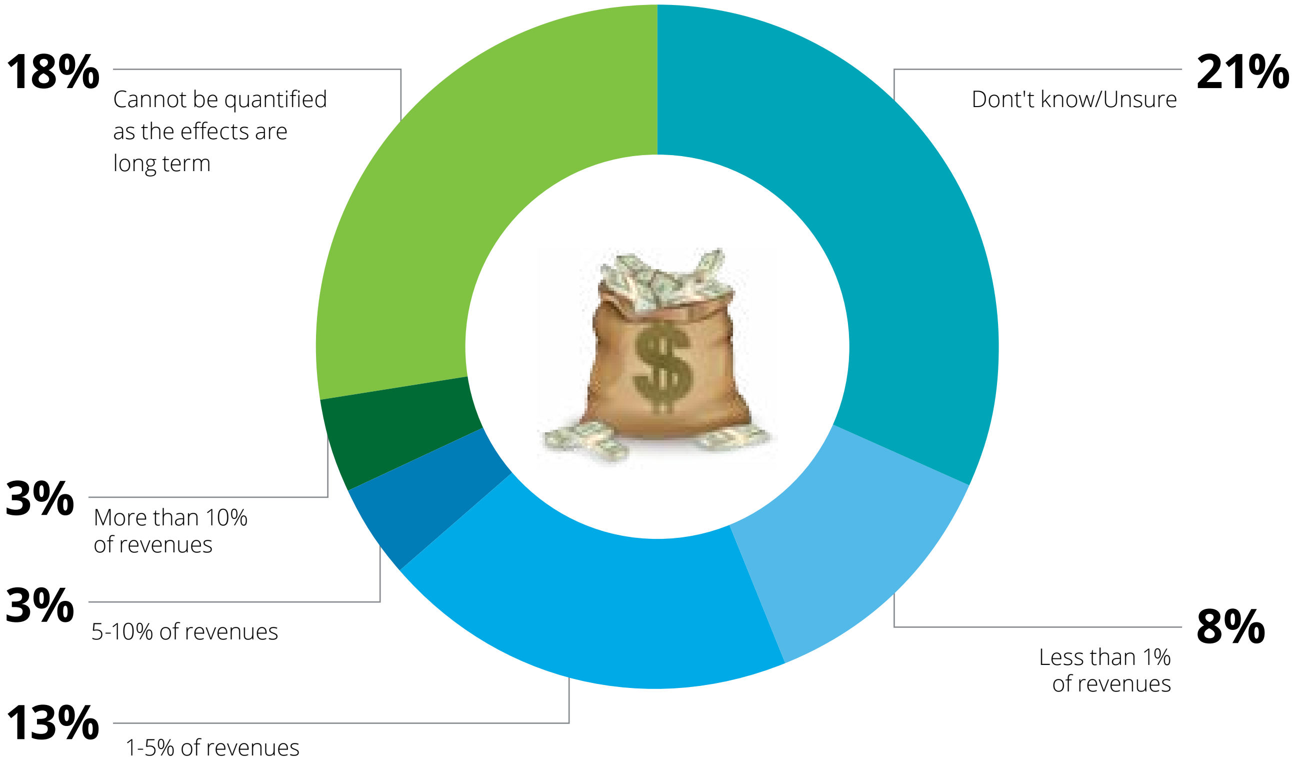
Note: This is a multiple choice question and responses will not add up to 100%

Rising regulatory focus by the Indian government is also building a case for a corruption free corporate India with 30% of respondents believing that stringent enforcement of anti-bribery regulations could end this menace.

Organizations are unable to tackle counterfeiting

Counterfeiting primarily occurs due to the inability of organizations to educate employees and customers on the potential damages of dealing with duplicates and counterfeit products. While, in the past, counterfeiting's primary impact was loss of revenue for organizations, today it has also extended to reputation in light of fierce competition for market share. In recent times, the proceeds from counterfeit products have also facilitated terrorist financing and anti-national activities. Accordingly, about 39% of survey respondents have indicated that they were unsure/unable to quantify the effects of counterfeiting.

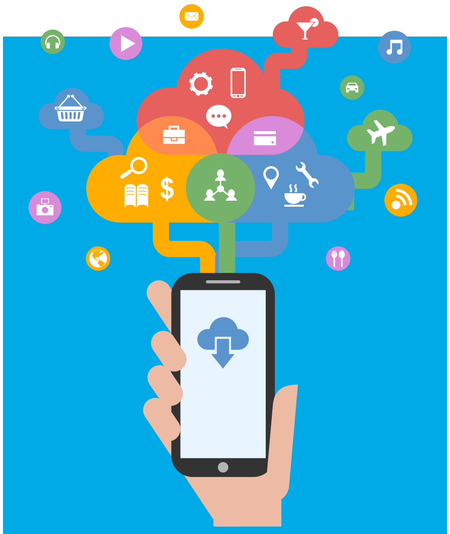
Figure 3: In your opinion, what is the perceived loss due to intellectual property (IP) theft and counterfeiting to organizations?



Note: 34% did not respond to the question.

According to survey respondents, organizations can take several measures to curb counterfeiting such as drawing up clauses specific to counterfeiting/IP theft in contracts, using third party experts to gather intelligence, and through employee education.

Point of View: Leveraging technology to curb counterfeiting
As consumerization in India grows, there is also an accompanied rise in the movement of counterfeit goods in the market. Several industry reports point to counterfeits amounting to at least 25 percent[3] of total goods circulating in the market across various product categories. While corporates are aware of this menace, efforts to curb counterfeits often tend to be inadequate. In our experience, investing in anti-counterfeit technologies may provide better safeguards against counterfeiting. Some options are discussed below.



Smartphone applications – These allow consumers to quickly check if an item is authentic prior to making a purchase. It also empowers brand owners to identify, track, and prevent brand infringers from selling counterfeit products. Typically, retail companies can put a Unique Product Identifier (UPI) on the product or on the packaging. Consumers can use their smartphones to scan the UPI. If the item is counterfeit, the system will notify the consumer that the product cannot be authenticated[4]. Some smartphone applications also allow users to take photos of possible counterfeits and upload them to an online map that's linked to a GPS locator[5]. This can alert other consumers of counterfeits in specific locations.

Radio Frequency Identification (RFID) – RFID can provide labelling technology like barcodes, but with greater capability. Barcodes typically encode product-labelling information like names and serial numbers, but nothing more. They require direct line-of-sight for access, can store only small amounts of information, and have minimum size requirements for effectiveness. As such, small sized items present challenges for item level barcode labelling. RFID technology, on the other hand, embeds labelling information in non-volatile memory devices, which in turn embeds in a product. Unlike barcodes, RFID tags come in various sizes (sometimes as small as a grain of rice), have greater storage capacity, and do not require direct line-of-sight for access. The absence of size and line-of-sight limitations allows RFID tags to embed virtually into any product for flexible labelling down to the item level. This capability enables automatic tracking and inventory control with strategically placed interrogators.

Working with digital marketplaces – The proliferation of ecommerce has been accompanied by a rise in online sales of counterfeits and duplicate products. However, unlike physical market places, it may be relatively easy to combat online counterfeit product sales, if organizations work closely with web platform providers. A simple move such as search engine optimization – where organizations invest to create content that promotes authentic products – can help consumers become more aware of authentic products, their features and pricing. Consequently, if search results start showing authentic products in the top listings, fakes tend to get pushed to the bottom where they may not enjoy visibility. Further, by adopting a more visible digital profile – such as having a web page with online sales capability, a Facebook page, Twitter handle, etc., brands can stymie efforts by counterfeiters trying to steal the ecommerce spotlight. Increasingly, ecommerce platforms are also blacklisting vendors providing fake products and initiating action against them [6].

Like many other fraud schemes, it is easier to prevent counterfeiting than to respond to incidents of large scale counterfeiting. The luxury products industry has successfully embraced some of these technologies and managed to curb counterfeiting to a significant extent. Other product companies can also explore these options and adopt those that are cost effective and user friendly.

[3] Source: http://indianexpress.com/article/india/india-others/about-rs-39000-crore-loss-in-one-year-due-to-illicit-markets-in-manufacturing-sectors-ficci-report/
[4] The Smart phone App 'Authenticateit' follows this technique to check for counterfeiting.
[5] Black Market Billions is a crowdsourcing app that operates with this technique.
[6] Source: http://fortune.com/2016/11/14/amazon-counterfeit-items-lawsuit/

Focus remains on mitigating known frauds

Overall, there appears to be little change in most of the trends discussed so far compared to our 2014 survey. Frauds identified as concerns have been limited to well-known categories such as bribery and corruption, theft and favoritism. Despite the changing business landscape and push to adopt technology in improving business outcomes, it is surprising to note that organizations continued to rate concerns such as cybercrime, IP fraud, e-Commerce fraud, and counterfeiting relatively low in terms of organizational impact. We believe this inexperience of new fraud risks could stem from limited understanding and the inability of organizations to detect patterns that may point to such fraud risks. If the current levels of fraud awareness were to continue, organizations may be unlikely to mitigate new frauds in the future.

Point of View: Organizations need to prepare for fraud arising from new business dynamics

In the last two years, three of the most significant fraud and reputational damage cases reported by the media arose due to social media exposure. These large global brands were questioned by consumers on their quality assurance practices, which upon investigation led to the discovery of noncompliance, malpractice and fraud. In two of these cases, the brands had to recall products from the market resulting in huge losses, and had to invest in brand re-building measures until consumers could regain faith.

Interestingly, these brands remain heavily invested in social media for customer engagement. Yet, they did not foresee the potential risks arising from this platform.

In our experience, large organizations in India continue to be saddled with legacy practices and tend to remain fixated on them–whether it is for business process improvements or fraud risk management. So, while one may see a very robust fraud risk management framework to prevent, say procurement fraud, there may be little or no steps taken to anticipate potential fraud in adopting e-procurement models. In theory, while e-procurement may not pose the same fraud risks as a conventional procurement process, and may be touted as the 'fraud free' frontier for the procurement function, practical experience can show otherwise. For instance, our 2014 fraud survey indicated online payments, procurement of materials, and trading in stock markets as areas vulnerable to fraud risks in e-commerce transactions.

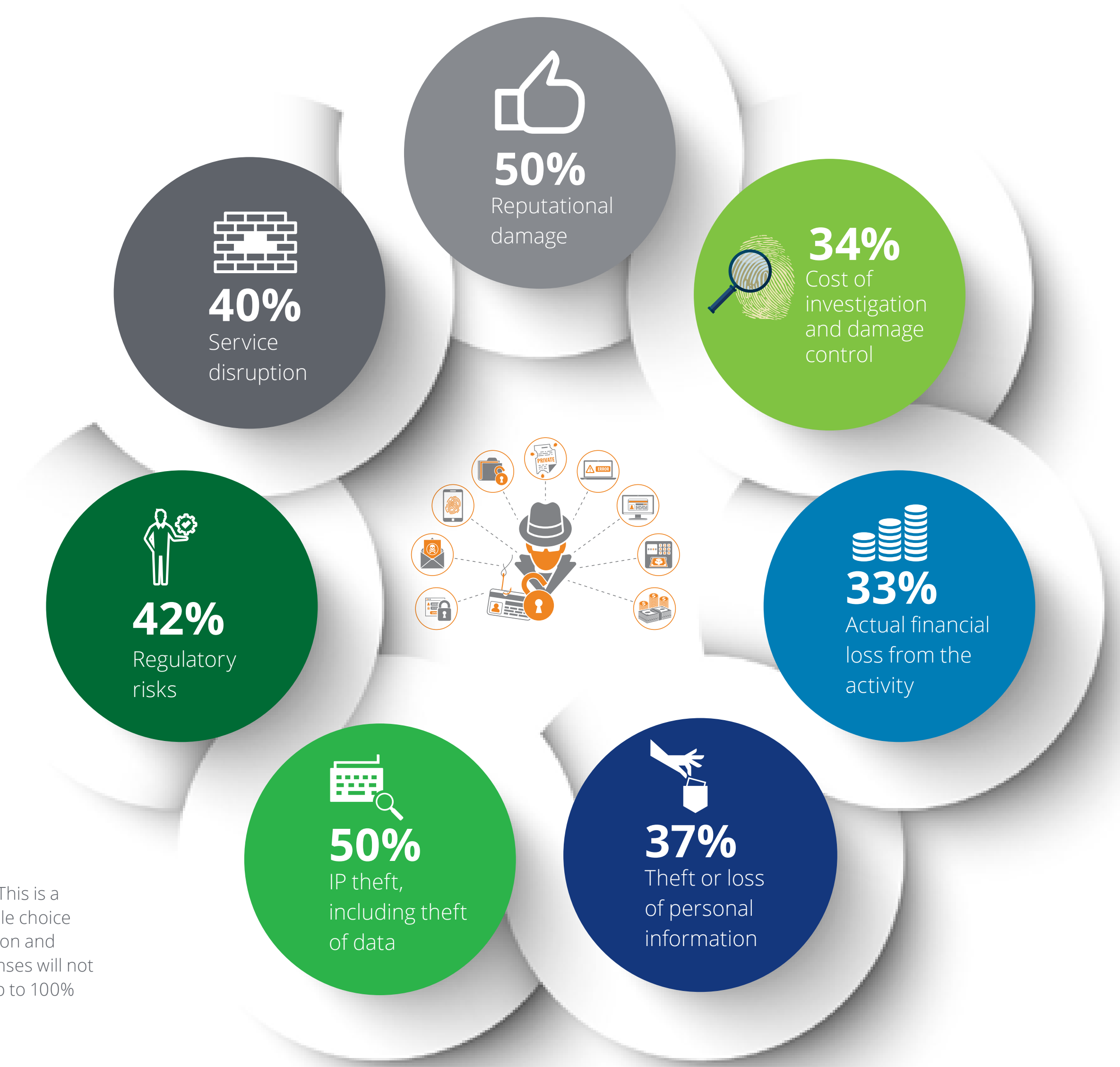
Further, in the past, organizations were aided by relative inaction from governments to bring about paradigm change in the way business was conducted. However, that appears to be changing today. The last two years have indicated a determination on the government's part to ensure ease of conducting business–whether that is by moving towards simplifying laws and tax structures or by pushing for cashless transactions. In such a scenario, organizations will experience new frauds, unless they proactively anticipate them and establish processes to mitigate these frauds.

Preparedness to tackle emerging fraud and regulatory noncompliance risks remains low

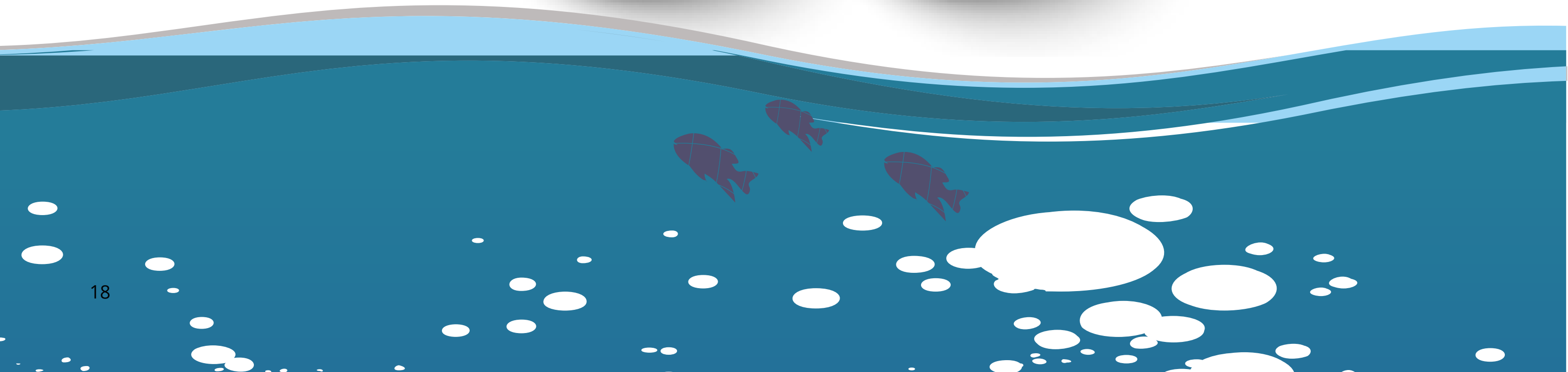
Limited understanding of cybercrime

Reputational damage, IP theft and regulatory risks, were identified as the most likely impact of cybercrime.

Figure 4: According to you, what is the greatest impact of cybercrime?



Note: This is a multiple choice question and responses will not add up to 100%



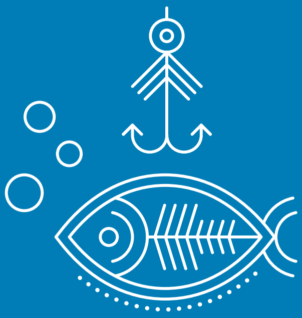
Considering the media has reported about organizations losing several million dollars to cybercrime globally, it is surprising to note that survey respondents rated financial loss from cybercrime low on the scale. We believe this could be due to the limited understanding of how cybercrime can manifest itself.

For instance, cloud computing fraud is one of the manifestations of cybercrime. 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. Our 2014 fraud survey states that only 5% of survey respondents indicated that their organizations had sustained losses from cloud-based intrusions. Around 43% 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. This is no different from what we observe today.

In the area of cybercrime prevention, majority of organizations still appear to be grappling with cybercrime, with a third saying they didn’t discuss the incident for fear of tarnishing their reputation. In our view, a clear plan to tackle cybercrime is the need of the hour. Such a plan would comprise of a responsibility matrix in case of an incident, root-cause analysis and situational diagnosis of the potential impact of the incident, and remediation plan. In many cases, the onboarding of specialist third parties for undertaking these activities is also documented in the response plan.

As the world moves towards increased adoption of digital technologies, it is imperative for organizations to become aware of the potential fraud risks involved. Failure to do so can result in business disruption.



Point of View: Hacking shows no signs of scaling down

This year the world has possibly experienced the largest number of large scale data breaches ever[7]. Many of these breaches–involving government departments as well as private organizations-were a result of hacking by third parties. Going by recent news, it is likely that such breaches and large scale hacking are becoming more common.

The economic drivers behind hacking have evolved dramatically over the years. In the past, hacking was done for amusement. Hackers focused on defacement (also known as hacktivism) to embarrass large organizations and their security set up. They would often black mail site operators with attacks that brought websites down (a "denial of service" attack), leading to the invention of the network firewall to stop this. However, as companies began digitizing organizational data on a large scale, hackers discovered that such data was worth a lot of money on the black market. Consequently, hacker focus has shifted in the last few years from denying service to stealing data.

There are various tools available today which can help hackers attack thousands of victims in just hours. Varieties of such tools and "ready programs" are available on the darknet[8]. Additionally, hacker forums tend to exemplify the spirit of web-based collaboration and education, offering a rich menu of tutorials, advice and technology designed to steal data.

Unfortunately, many organizations have been unable to keep up with the advancements in the hacking ecosystem and remain equipped with old cyber security models designed to keep the 'hacker-of-the-90s' out. This needs to change; organizations need to invest in building a robust preventive framework. Such a framework must include the following:

Data protection: Developing a robust data classification regime that restricts data access to very few employees can be a start. Several large organizations already restrict access to data around financial information, employee information, business plans and client details. Alongside this, organizations can also limit the transfer of data to reduce potential access points for hackers to invade internal systems.

Subscribing to suitable and up-to-date protection tools which can block links to known malicious sites can prevent access at an enterprise level. Further, encryption must be strongly recommended for all devices accessing organizational networks for data.

Continuous monitoring of internal controls can help identify potential instances of data leaks or breaches, as well as suspicious activity.

Focused training programs – Organizations can segregate their employees into different user groups based on the information they are privy to such as those in the procurement function, finance and accounts staff, customer relationship team, sales team, etc. Depending on the level of information these employees hold, focused training programs must be organized to help them recognize potential hacking scenarios and avoid them. Further, any known instances of hacking attacks can be shared throughout the organization to warn employees. A leading best practice is to have the IT security team share this information alongside recommended actions.

In addition to a preventive framework, organizations must also invest in a cyber incident response plan to prevent large scale hacking. This includes conducting a comprehensive forensic readiness assessment, investigation to understand the potential scale of the incident, assessing the damages caused based on the data that was sought, and having a remediation plan, including root cause analysis.

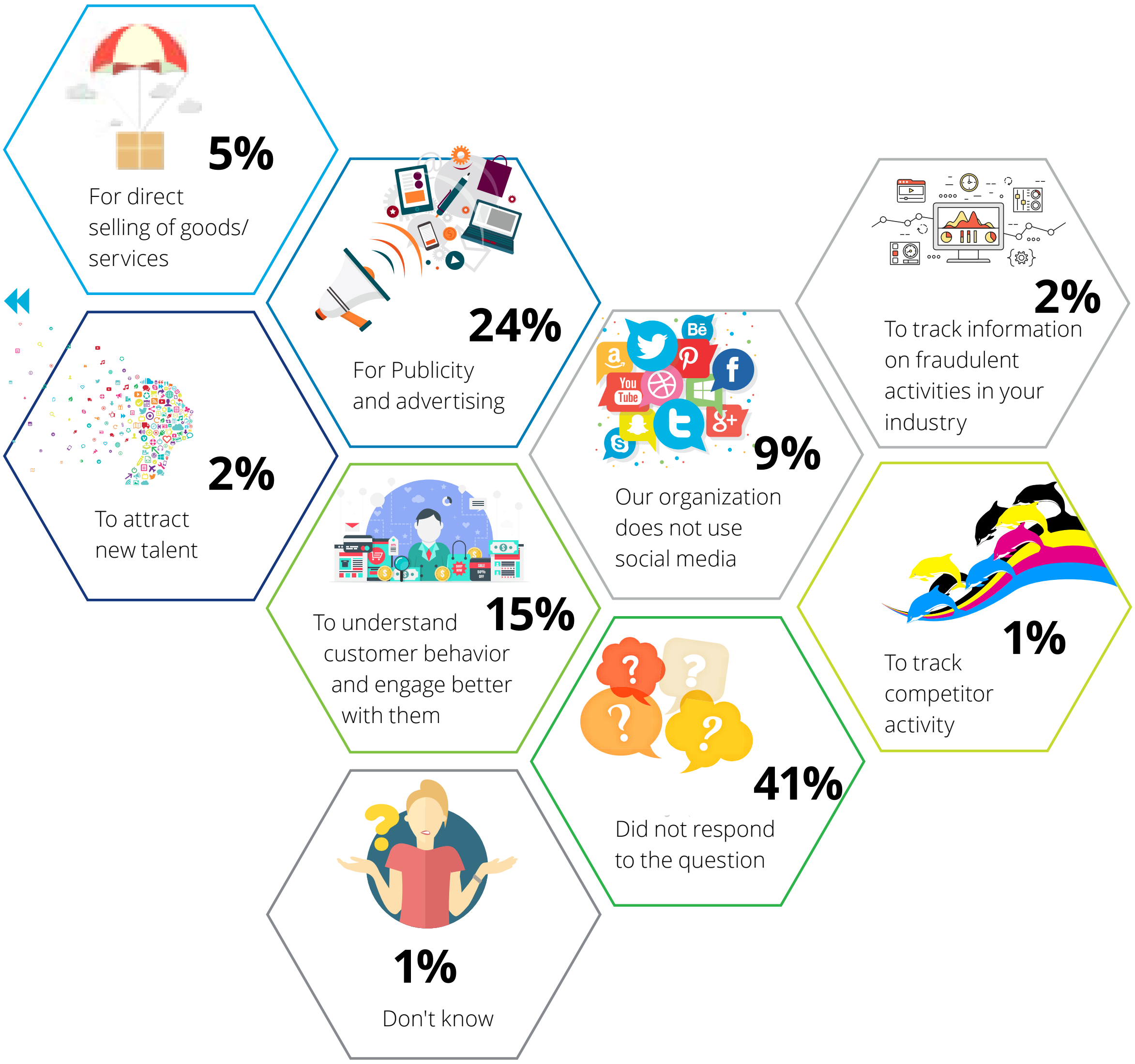
As organizations mature, there is bound to be increased reliance on digital platforms to host data. Without the right security measures, these data platforms are likely to invite new age hackers.

[7] Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
[8] A darknet is a computer network with restricted access that is used chiefly for illegal peer-to-peer file sharing.

Social media–to be or not to be on it–remains a concern

A majority of survey respondents did not respond to the question of why their organizations used social media. Among those respondents that did, the majority said their organizations used social media for publicity and advertising, followed by understanding customer behaviour and engagement.

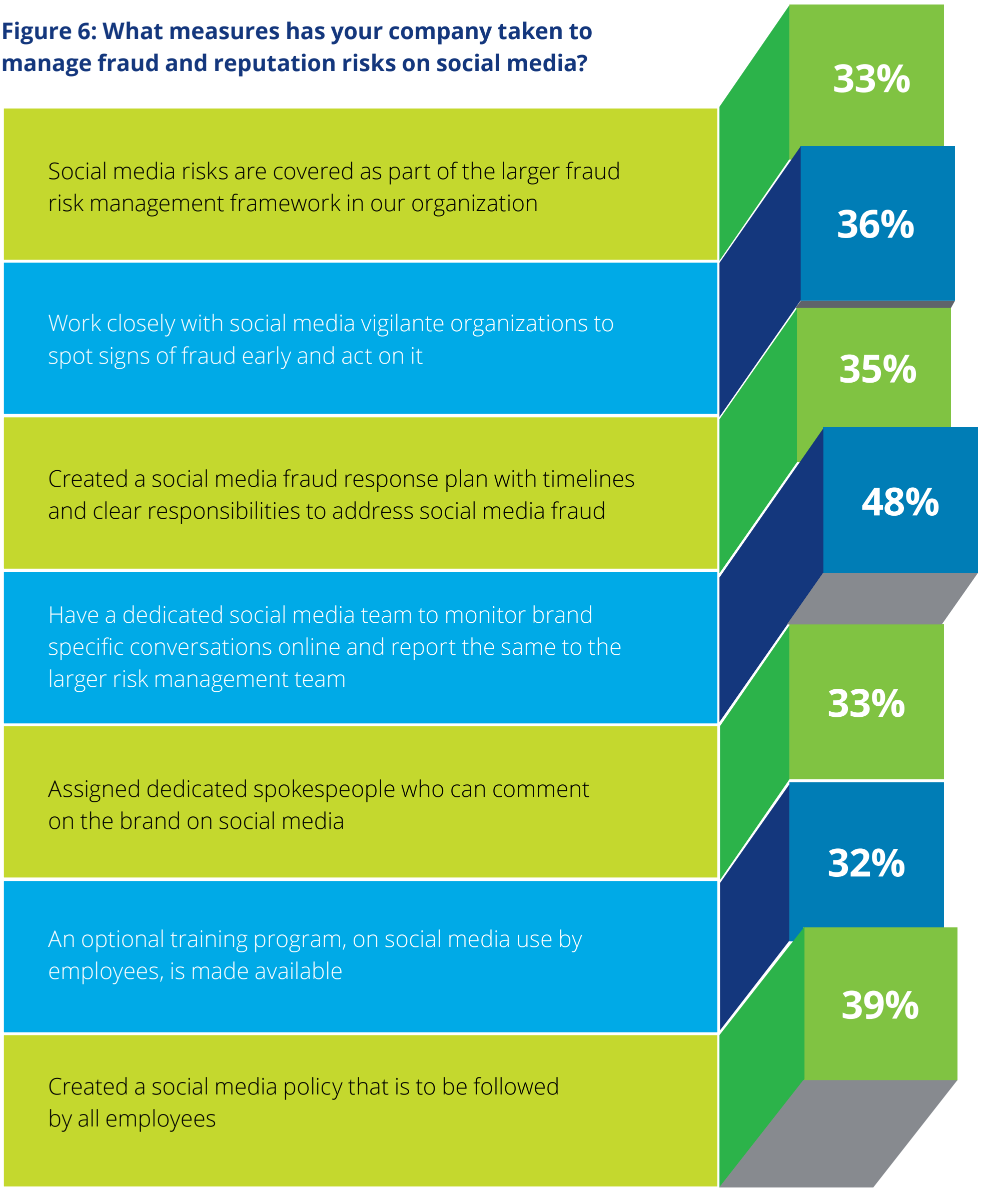
Figure 5: What is the primary purpose of your company using social media?



When asked to identify the fraud risks that their organizations faced on social media, respondents pointed to misuse of intellectual property by unauthorized users (68%), and use of fake profiles masquerading as the company to fool customers (65%). Both of these situations can result in loss of confidential information–both belonging to the company and to customers–that can be misused for monetary gain by fraudsters.

To manage fraud risks on social media, a majority of respondents said they relied on a dedicated social media team to monitor brand specific conversations online, reporting concerns to the risk management team. Creating a social media policy for employees to follow and working with social media vigilante organizations to spot fraud early were identified as the other common measures adopted by organizations.

Figure 6: What measures has your company taken to manage fraud and reputation risks on social media?



Note: This is a multiple choice question and responses will not add up to 100%

When asked how they reacted to being confronted by a smear campaign, most respondents did not respond. Among those who did, 27% said they engaged with their audience by providing facts and sharing status updates on how the issue was being dealt with. Another 13% said they did not use social media, but conventional media such as advertisement or press release, to respond to smear campaigns. These sentiments indicate that organizations appear to view social media as yet another channel for communication, not very different from conventional media. There also appears to be a strong desire to control social media and drown out voices of dissent. In our experience, this may not help organizations in the long term.

Point of View: Controlling the uncontrollable – How organizations can stay safe on social media

Many organizations are choosing to have a social media presence today in order to capitalize on its potential for inexpensive, large scale communication–whether it is to further a cause, generate publicity, or generally be noticed by specific target groups. The genesis of social media lies in promoting free thought and communication. Unfortunately, this very fundamental tenet tends to pose significant fraud and reputation risks for organizations.

For starters, verification of facts prior to posting information tends to be overlooked in the rush for being the 'first to post'. This can result in the rapid spread of misinformation, which can be difficult to curb. Recently, social media in India has witnessed significant polarization of views pertaining to many current topics – whether it be the release of certain films (possibly influencing stock prizes of the organization producing the movie), the government's move towards demonetization of currency, and organizational performance in B2C companies in light of festival season sales. In other instances, customer complaints on social media have gone viral, with people trolling the company's accounts, thus preventing a chance for resolution.

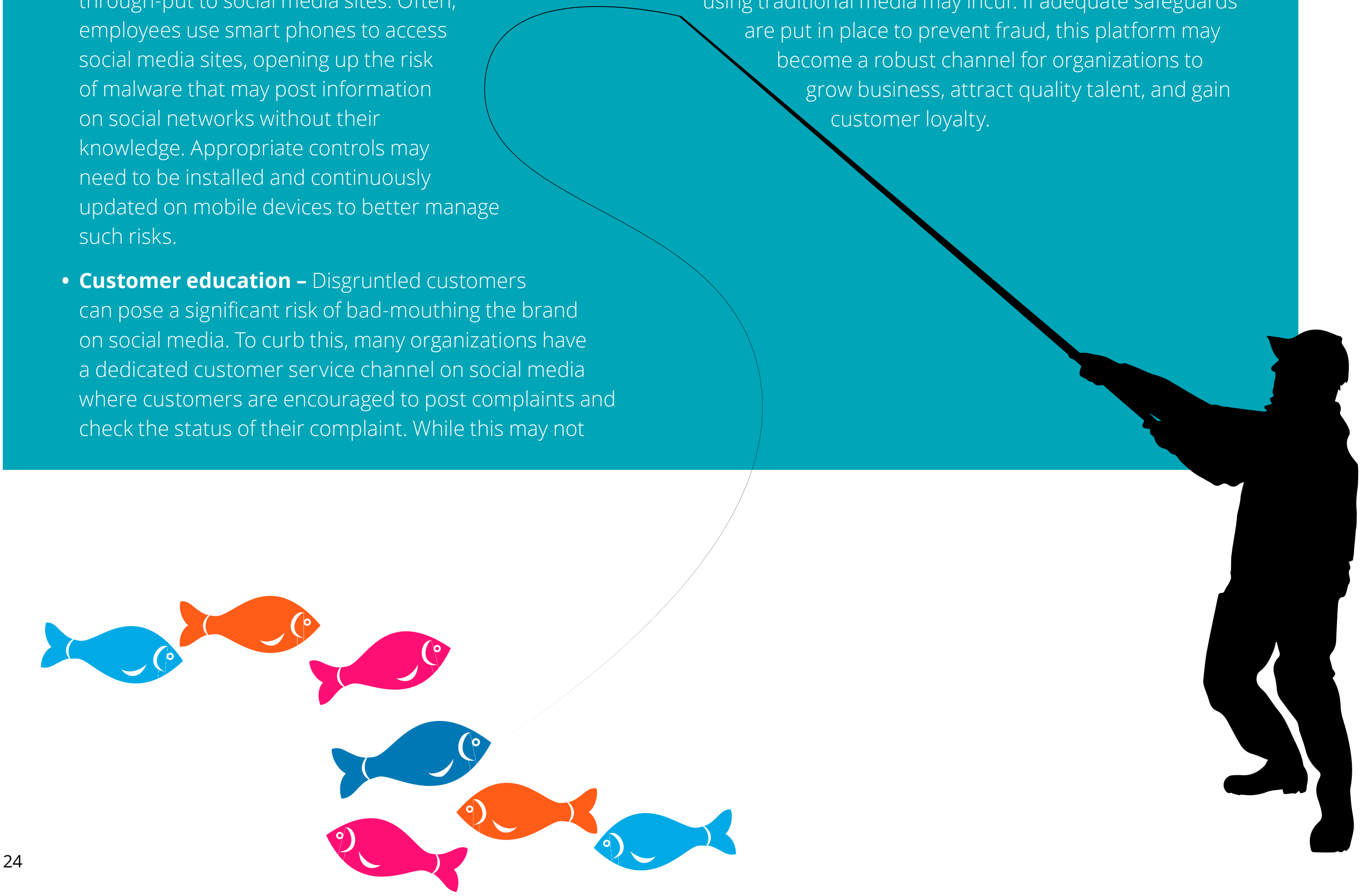
There have also been cases where fraudsters have created fake social media profiles offering job opportunities on behalf of organizations, which may be unaware of such misuse of their brand. Unethical competitors can run campaigns using fake accounts posing as consumers or reviewers posting unfavourable product/service reviews. Yet another example of social media fraud is identity theft. We have observed that fraudsters use social media platforms to steal personal information and use it to access financial information. Such frauds can be committed from anywhere around the world, making it difficult to identify the fraudster(s).

We have also observed cases where confidential information pertaining to business plans, financials and intellectual property was released on social media by fraudsters. In these cases, privacy laws tend to have limited effectiveness because these confidential documents may likely reside in cloud storage systems making it difficult to limit the number of infringed copies. Further, social media networks often change their privacy settings and unless users monitor this carefully, they may inadvertently reveal confidential information to all users of the platform.

Removing offending posts on social media is difficult and, many times offense may appear to be the only defence for organizations. In our experience, the following measures may help organizations safeguard themselves from social media fraud.

- **Monitoring the brand for misuse of brand name –** There are tools available to monitor brand mentions and brand sentiment on social media. These can help understand how the brand is perceived and take corrective action wherever necessary. Often, such action can prevent undesirable information from going viral.
- **Training and awareness for employees on social media use –** Clear guidelines on what content is permissible for social media sharing, who is authorized to comment on the brand in their official capacity, disclaimers that employees must use on their personal profiles to isolate risks to the brand, etc. must be outlined. Further, a dedicated training program outlining common scenarios that result in information compromise on social media can help employees understand the potential implications of their actions.
- **Managing employee accessibility to social media sites** through content filtering or by limiting network through-put to social media sites. Often, employees use smart phones to access social media sites, opening up the risk of malware that may post information on social networks without their knowledge. Appropriate controls may need to be installed and continuously updated on mobile devices to better manage such risks.
- **Customer education –** Disgruntled customers can pose a significant risk of bad-mouthing the brand on social media. To curb this, many organizations have a dedicated customer service channel on social media where customers are encouraged to post complaints and check the status of their complaint. While this may not be practical for all organizations, educating customers on the best possible way to resolve complaints may help reduce instances of negative coverage on social media. For instance, organizations can provide a confidential space on social media–like a closed group that encourages private conversation–to report issues with their brand.
- **Having a social media fraud response plan –** Organizations may not always be able to prevent social media fraud, but they can be better prepared to deal with it. Having a reaction plan and corresponding timelines to deal with well-known instances of social media fraud may help limit the spread of misinformation and control the damage. Such a plan can include a list of actions that the organization can take when confronted with social media fraud or reputational damage. This can include the process to investigate the issue and timelines for identifying the root cause(s), procedures for on-boarding of third party experts to investigate the issue (should the need arise), guidelines on communication to clients and employees to quell fears, and maintaining a list of authorized individuals who can coordinate the organization's response and post it through official channels.

Social media provides an opportunity for organizations to improve their customer reach at a fraction of the costs that using traditional media may incur. If adequate safeguards are put in place to prevent fraud, this platform may become a robust channel for organizations to grow business, attract quality talent, and gain customer loyalty.



Anti-competitive behavior – Are you covered?

The last two years have seen rising legislative action by the Competition Commission of India (CCI). Companies have been collectively levied fines ranging from a few crores to as much as several hundred crore rupees for violating the principles of competitive behavior outlined in the Competition Act. This exposes organizations to a relatively newer risk in the Indian context–that of their growth strategies and consequent business actions being scrutinized for inappropriate behavior in regards to competition.

That this is a relatively newer risk in the Indian context is corroborated by the responses in our survey wherein a large number of respondents have either chosen not to respond or have chosen 'not sure'/'don't know as a response. Clearly, a greater degree of awareness needs to be created amongst businesses for requirements under the Competition Law and make them have robust compliance processes.

Figure 7: Do you believe your organization can be pulled up for anti-competitive behavior by the CCI in the near future?

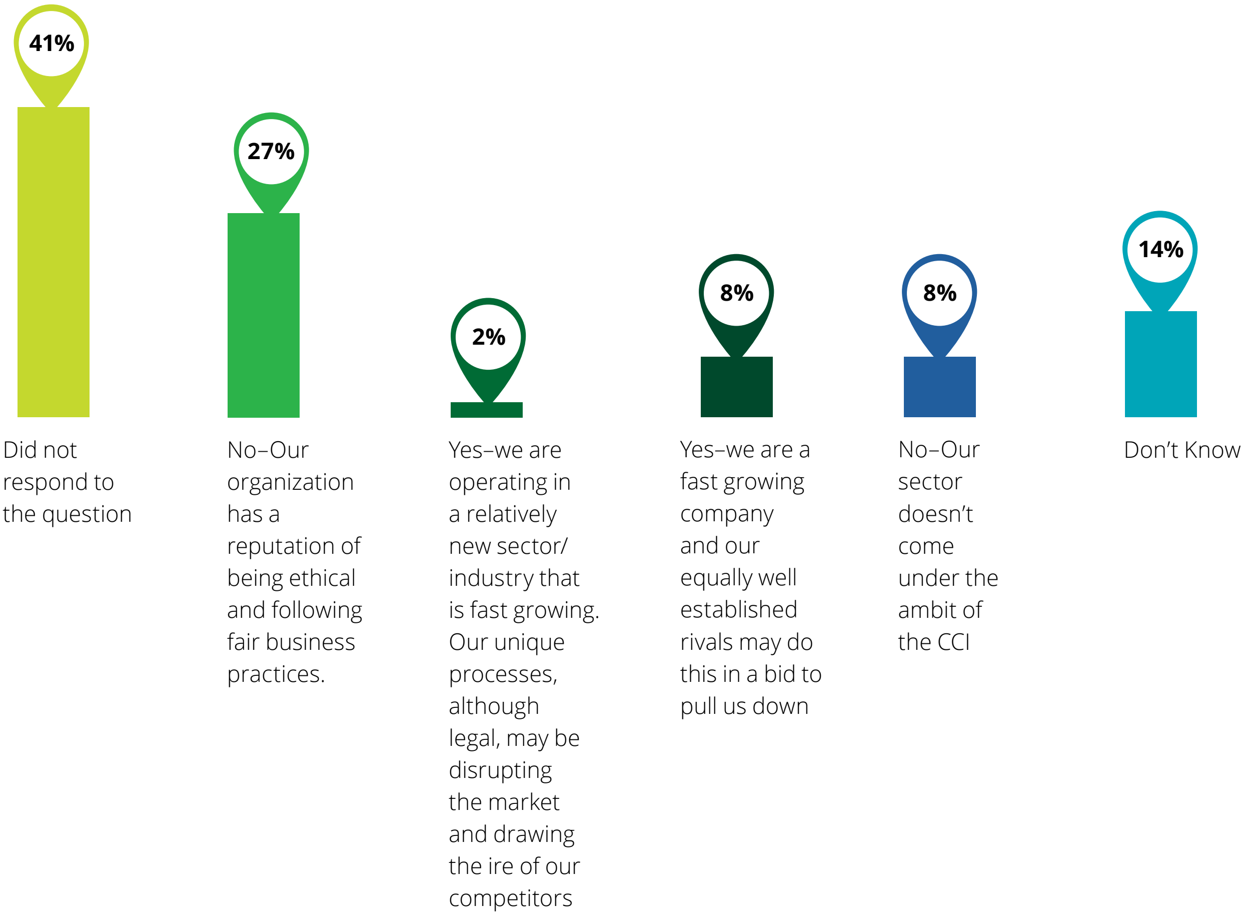
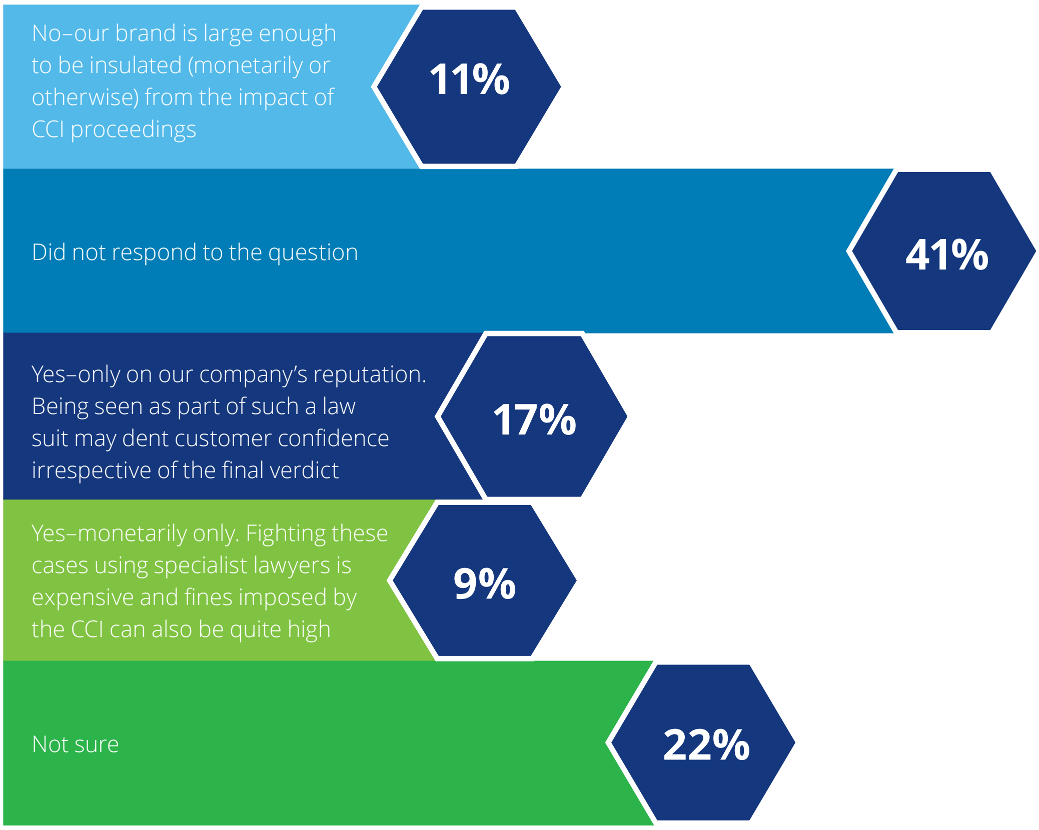
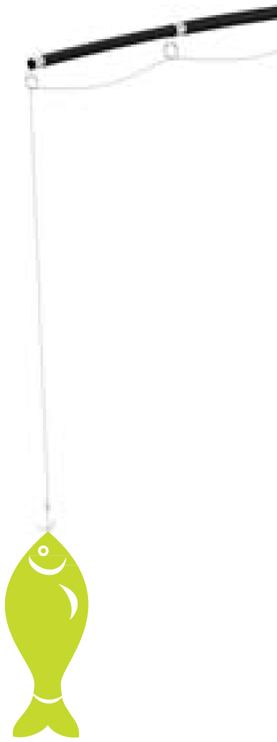


Figure 8: In your opinion, does being part of an anti-competitive behavior law suit have a significant impact on your organization?



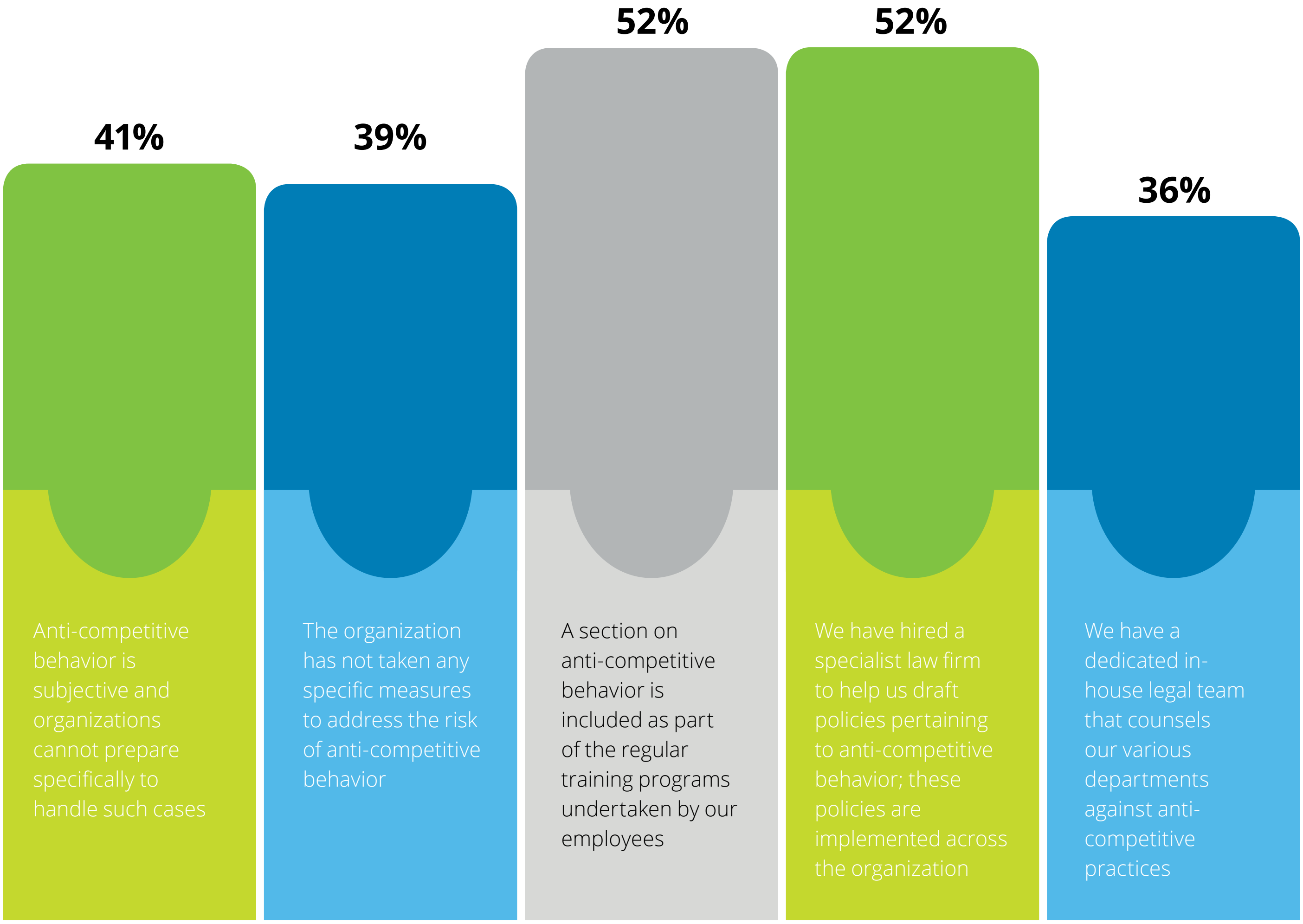


There appears to be lack of understanding of the risk emanating from non-compliance to Competition Law as also about what actions/behavior may constitute an anti-competitive behavior under the Law. Most respondents to the survey believed they were unlikely to be impacted by a CCI investigation whereas many others were unsure when asked if a CCI law suit would have a significant impact on their reputation.

Indian businesses will need to take this law seriously else they risk significant penalties being levied and their reputation being adversely impacted. The Competition Law redefines business conduct and some of the traditional ways of doing business may now be looked upon as unacceptable business practices. There has been a significant increase in the number of information filings with CCI as well as the number of investigations that it is carrying out. The CCI has levied fines of more than USD 2 billion over the past five years.

Compliance with the requirements of the Competition Law is a subjective matter that can be extremely complex. Hence, there seems to be some confusion in the minds of survey respondents while responding to our question with regards to compliance measures. When asked how organizations addressed potential risks arising from non-compliance to the Competition Law, respondents shared mixed reactions. One set of respondents indicated hiring specialist law firms to help draft policies pertaining to anti-competitive behavior and including a section on anti-competitive behavior as part of employee training programs. Another set of respondents said their organizations had taken no specific steps and that anti-competitive behavior was subjective, making it difficult to prepare to handle such cases.

Figure 9: What measures has your organization taken to address the risk of anti-competitive behavior?



Note: This is a multiple choice question and responses will not add up to 100%

Point of View: Mitigating chances of a CCI inquiry – Some steps for consideration

To avoid punitive action under the Competition Act, Indian business organizations need to evolve a strong culture of compliance covering increasing awareness about the requirements of law, robust code of conduct, promoting fair business practices as also individual conduct while interacting with competitors. Some specific considerations include:

- Seek employee undertakings with regards to compliance with the Competition Act
- Develop an anti-trust law compliance manual – Such a manual should ideally contain the following: introduction to the Competition Act and key requirements under the law, outline businesses, business processes and key personnel that carry high risk; do'-s and don't'-s for the employees, expected behaviour while dealing with competitors, suppliers, dealers, traders etc.
- Create better awareness through regular training programs for competition law compliance – A broader programme should be designed for all employees and specific programs can be developed for key business roles that have higher perceived compliance risks (teams who interact regularly with the competition, customers and suppliers). These programs should be focused on educating the participants on potential infringements and how to avoid them. Some examples of infringements include, salespeople generally buying "shelf space" for their products and imposing restrictions on wholesalers and retailers. This kind of conduct is exclusionary in nature as it prohibits the wholesaler/retailer to stock competitor's product. Other examples include informally discussing prices and promotional schemes with competitors at industry events or social gatherings. Ideally, such training programmes should be conducted every six months and reviewed annually.
- Closely monitoring business information shared at meetings with trade associations, which bring together key competitors. At the very minimum,the agenda of any such meeting should be vetted by the legal counsel of the company and details of the meeting's discussion should be shared with the legal counsel.
- Review all trade association memberships and prepare specific guidelines for participation in such meetings
- Conduct mock raids to sensitize employees to the possibility of sudden scrutiny by the regulator.

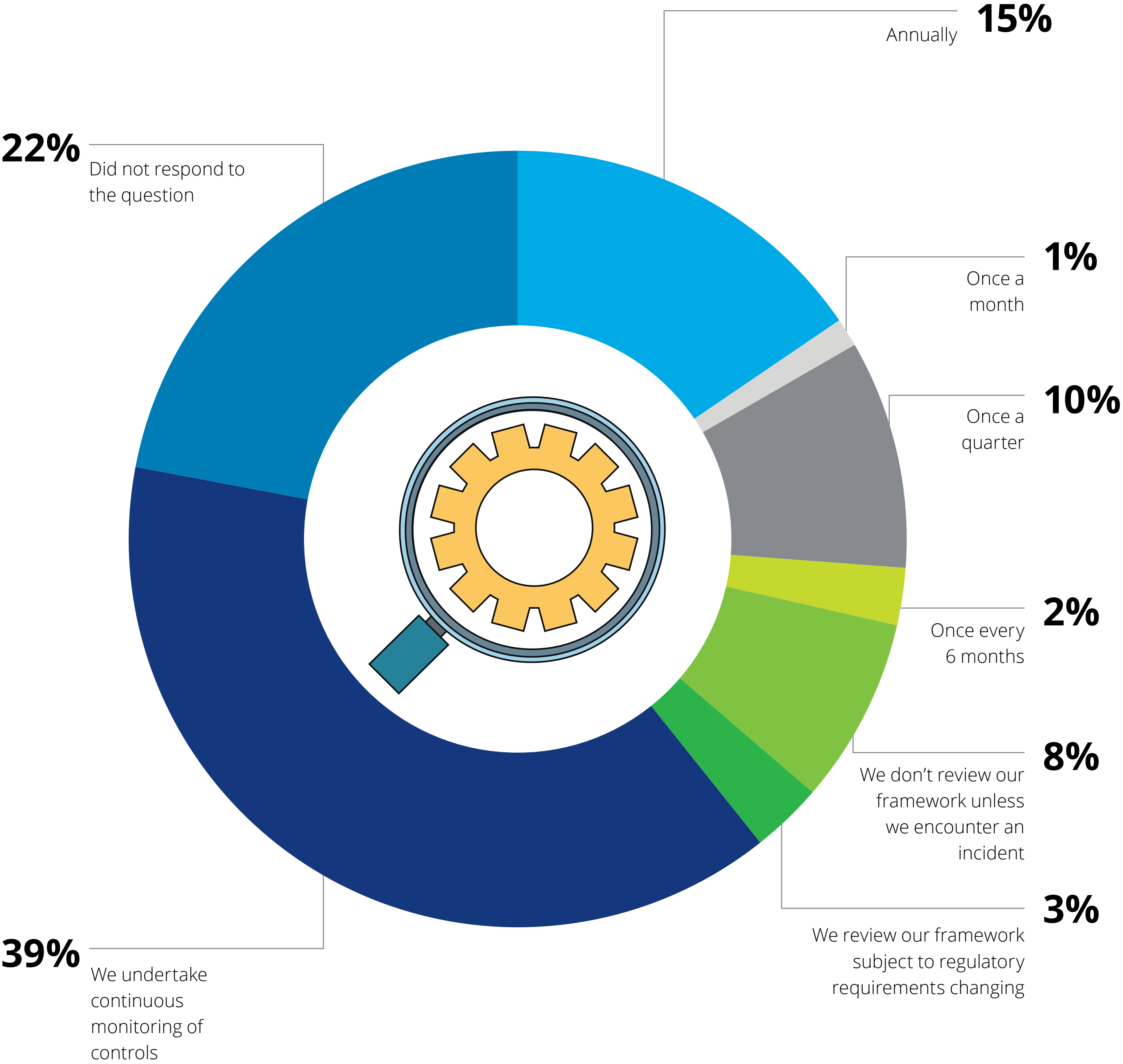
Conventional processes dominate overall fraud prevention, detection and response strategies

There are mixed reactions on who shoulders the responsibility of fraud risk management, with respondents indicating that the Board should be responsible for fraud prevention, whereas the Internal Audit team should be responsible for fraud detection and investigation.

While leading practices and our own experience indicate that the Chief Financial Officer (CFO) and the Chief Risk Officer/ General Counsel undertake primary accountability for fraud risk management, changing business and regulatory landscapes mean other stakeholders need to assist these primary stakeholders wherever appropriate. For instance, in the information technology industry, the role of the Chief Information Officer (CIO) and Chief Information and Security Officer (CISO) becomes important in case of cybercrime, and these individuals and their teams need to support the CFO in getting information pertaining to the incident, as well as help plug gaps in internal controls. Similarly, in the real estate business, procurement is a significant fraud risk that is fraught with legal complications and hence the Legal Head may have to support the CFO in information gathering and resolution of potential fraud. In the Pharma industry, the Chief Compliance Officer usually assists the CFO wherever there are allegations pertaining to regulatory noncompliance.

Irrespective of who has the primary responsibility to manage fraud risks, it is important for a robust system to be in place to review fraud risk management measures. It is heartening to note that 39% of respondents indicated that their organizations undertook continuous monitoring of controls. However, organizations must also ensure that controls are periodically updated in line with the business landscape and knowledge of potential frauds, failing which they may not be able to prevent new frauds. As new data gets generated within organizations, an automated system of continuous monitoring is the way forward.

Figure 10: How often do you review your fraud risk management measures?



Point of View: Automation is the future of fraud risk management

A fraudster is always one step ahead and with technological advancements, he/she is also developing newer ways to perpetrate sophisticated fraud schemes that appear difficult to detect or prevent. Recent instances of large scale hacking and social engineering are indicators of what technology, in the hands of fraudsters, can result in. To stay ahead of the curve, organizations need to invest in the next generation of automated fraud risk management measures to ensure safety.

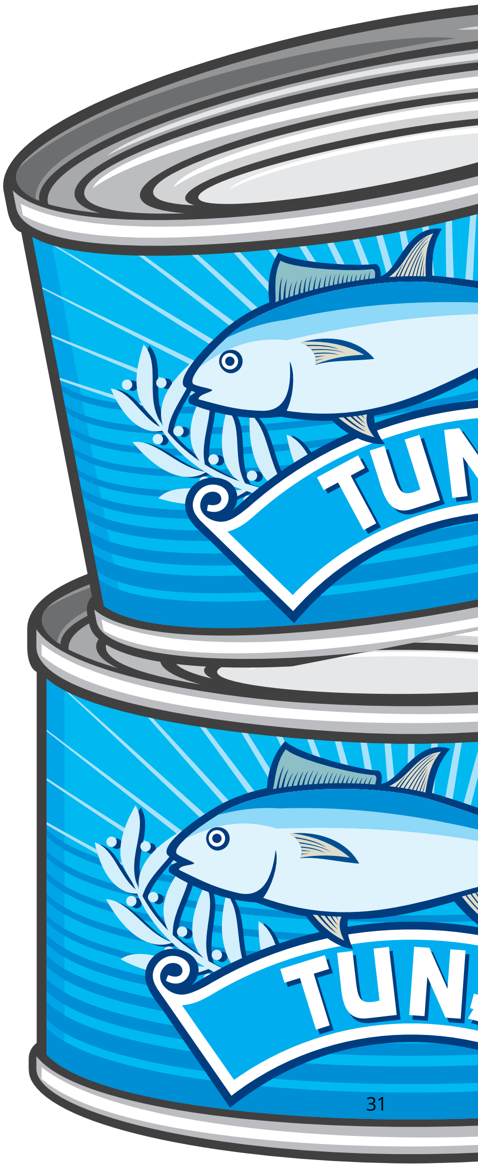
Historically, most organizations have built home-grown systems that use business rules to manage their fraud detection processes. These hand-crafted rules which are framed as "if-then" statements are called Robotics Process Automation (RPA) techniques. An example would be: "if several transactions are made within a short amount of time in a different state, then send the account for manual review" or "if an isolated transaction takes place by using a customer's credit card from a country other than what is mentioned in the registered address, then send this transaction for further screening". These rules have been built and refined based on decades of manual experience of analysing fraud data. Many of these rules are set up to provide additional analysis for unusual transaction behaviour. Although proven to be very useful, particularly for the e-commerce and m-commerce industries, RPA techniques tend to work efficiently primarily in a structured data environment.

In today's day and age, however, the amount of data being produced and the complexity of analysis has grown to unprecedented levels. This is making the manual process of building and maintaining business rules expensive, time intensive and less predictive. This is where, we believe, machine learning technology can be useful.

Machine learning uses computer systems with artificial intelligence capability to autonomously learn, predict, act, and explain without being explicitly programmed. This means the computer can learn from the outcomes of analysing existing data, and those learnings can then be applied to newly generated data to provide insights. This can be better understood through the example of online chess. A computer which either wins or loses, assigns a value to the series of winning moves it used during that game. After playing several such games, the system can predict which moves are most likely to result in a winning situation.

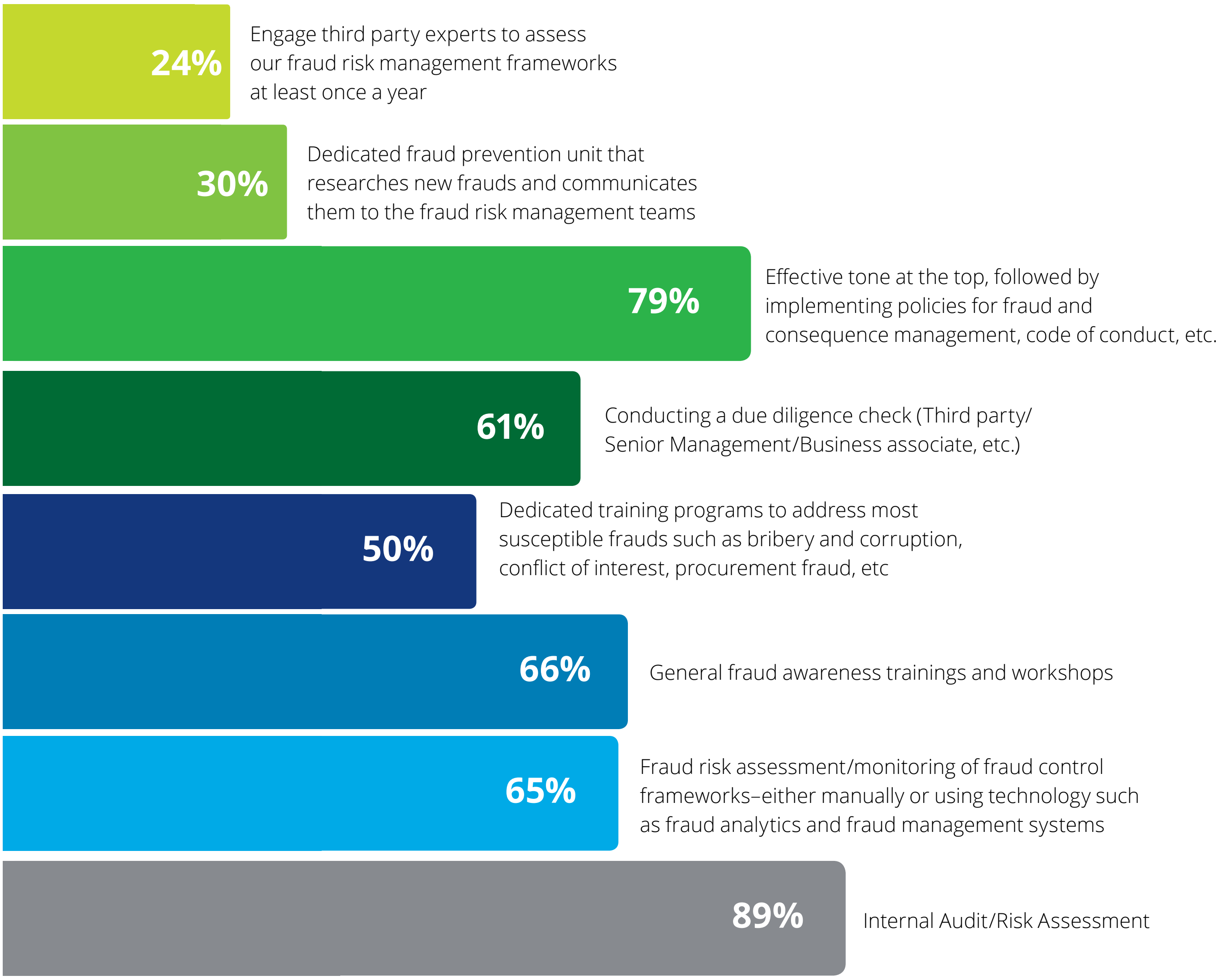
Similarly, a machine learning system could learn to distinguish between suspicious transactions (which are potentially outside the normal patterns of activity) and legitimate ones. Further, machine learning can also analyse big data more efficiently, build statistical models quickly, and react to new suspicious behaviours faster.

Machine learning can also be extended to multiple environments such as ecommerce and m-commerce to prevent and detect frauds. These systems can scale up to meet the demands of big data with greater flexibility than traditional methods used for fraud prevention and detection. We are already seeing increasing implementation of machine learning systems at banks and it is a matter of time before this becomes widespread across other industries. We believe the advent of machine learning for fraud prevention will change how organizations manage their fraud risk programs. Human oversight and intuition will remain critical to success, but machines will increasingly do the heavy lifting.



In the area of fraud prevention we are seeing a rise in preference for conducting due diligence prior to onboarding business partners. This is a welcome change, but can also be a challenge for companies considering India still has a very fragmented data regime, posing a challenge for companies seeking details for due diligence. Depending on the scope of relationship sought with the business partner, due diligence needs may be outsourced to specialist organizations.

Figure 11 : What measures does your company adopt to prevent incidents of fraud?



Note: This is a multiple choice question and responses will not add up to 100%

Point of View: The Importance of Due Diligence

Companies today need to be agile and efficient to remain viable, and this calls for co-operation, collaboration, and delegation to achieve business goals, resulting in a complex network of business relationships that can be fraught with numerous risks. Regulators around the world are increasingly taking a strong stance against questionable practices–holding organizations responsible for any unethical activities that occur within their sphere of influence. This is exemplified in the stringent provisions under the UK Bribery Act and the US Foreign Corrupt Practices Act.

Whether seeking to invest in a promising enterprise, forming a joint venture with a business partner, engaging a vendor, or taking on a large client, organizations need to exercise due diligence to ensure that these prospective partners possess the requisite capabilities to fulfil their commitments. Additionally, organizations need to ascertain if these prospective partners have a history of poor performance, litigiousness, and fraud; or reputational issues such as political exposure or links to organized crime which could adversely impact their reputation.

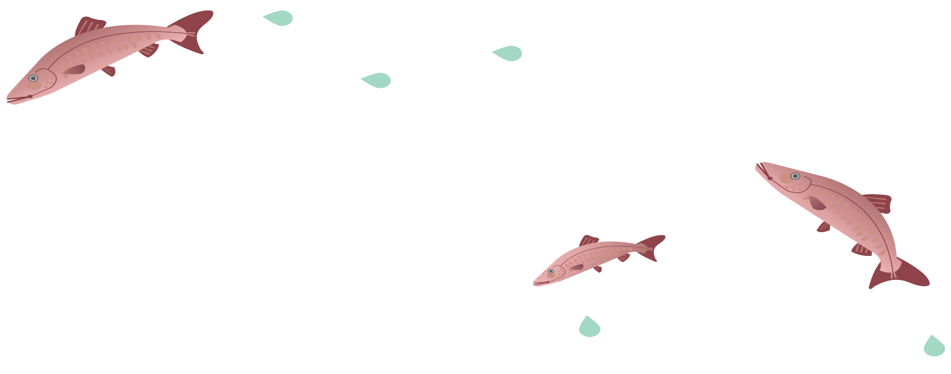
While experts familiar with industry practices and dynamics will be able to perform a technical appraisal of prospective partner organizations, a skilled due diligence specialist can uncover issues that can be hidden wilfully. In our own experience, quite a few entities that our clients have regarded to be 'clean' have frequently been found to have 'multiple skeletons hidden in their closet'. Political exposure, conflicts of interest, undisclosed related parties, undisclosed litigation, bankruptcy, sanctioned operations, unknown Ultimate Beneficial Ownership, diversion of business and outright fraud have been some of the issues that we have discovered.

Apart from engaging with enterprises, associating with individuals also requires due diligence. Respondents to our 2014 survey indicated that members of senior management were most likely to commit fraud. This underscores the importance of looking into the antecedents of potential candidates for high-level jobs. In our experience, senior management due diligence, has frequently revealed issues such as conflicts of interest, adverse reputation, allegations of malfeasance, negative personality traits, and fabricated work history in individuals who would have otherwise been appointed to positions of great responsibility. For closely held or family-controlled enterprises, it is particularly important to determine if the incumbent will be a good fit in the company's culture. Hence, due diligence should form a critical component in hiring members of senior management or Independent Directors for company boards.

As business grows and strategic partnerships are formed, it is crucial that organizations engage with a due diligence specialist to better mitigate fraud risks arising from counterparties.

The below table discusses three situations where a due diligence specialist can help protect business.

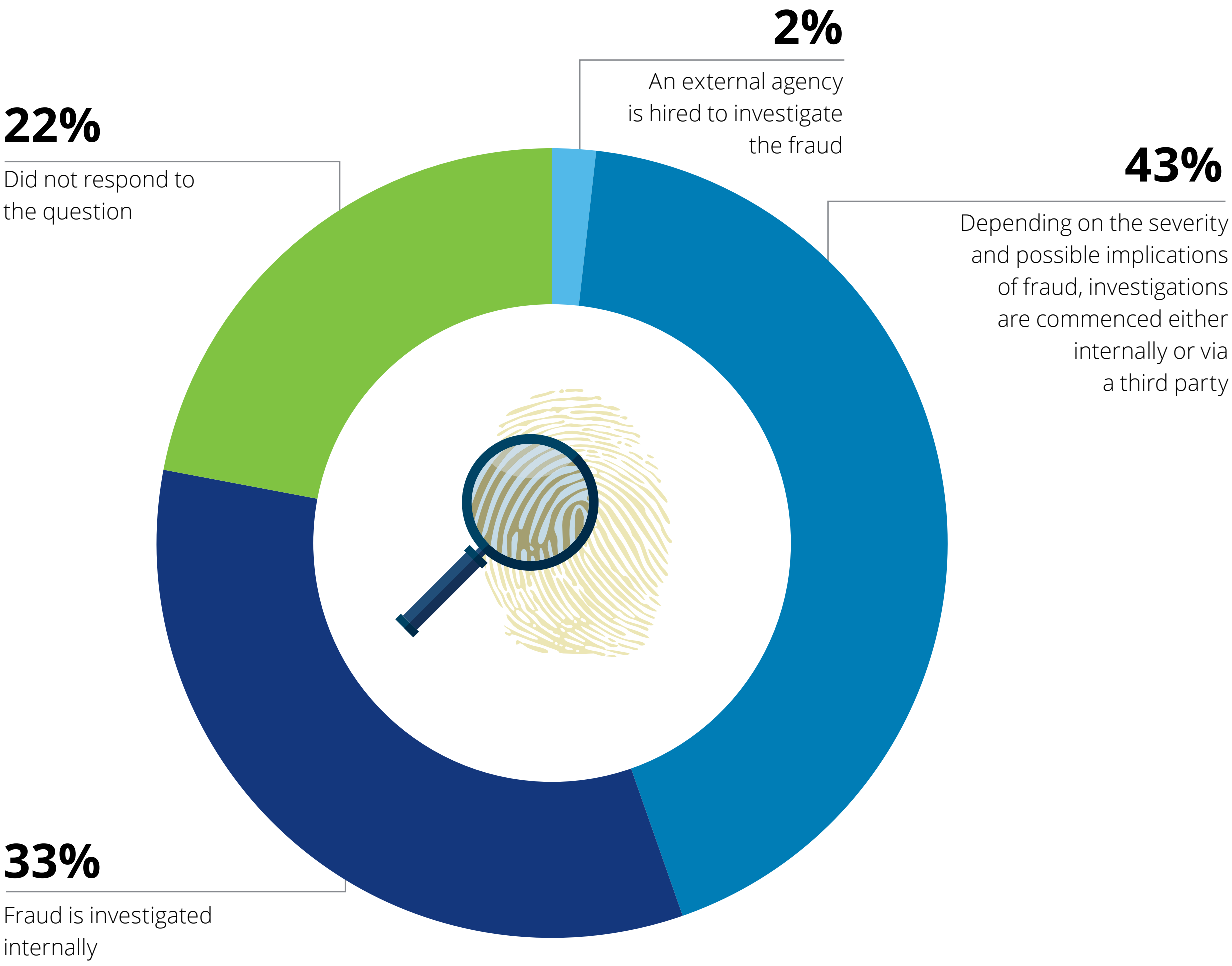
Situation	In-house Due Diligence	External Due Diligence Specialist
Merger or acquisition	• Dependence on publically available information and financial statements • Anecdotal feedback from personal networks	• Detailed feedback on public profile • Track record of the entity and key personnel along with history of dealing with multiple stakeholders • Litigation and regulatory searches for hidden liabilities • Source enquiries to scan for unethical activities, business practices, fraud, or adverse reputation
Recruiting a C-Level hire	• Overt reference checks	• Litigation and regulatory checks • 360 degree feedback encompassing employment verification, professional skills, workplace reputation, personality traits and temperament • Detailed analysis on reasons for leaving previous employers to determine if adverse events were present
Engaging a vendor	• Supporting documents as part of tendering process • Publically available financial statements	• Specific feedback on technical and financial capabilities through source enquiries • Market reputation and prevalence of unethical practices • Identify potential conflicts of interest • Site visits as required



In the area of fraud detection, organizations continue to rely on internal audit and whistleblower hotlines. This is in line with our 2014 survey results. What is different is the response to fraud.

A majority of respondents said they investigated concerns both internally and/or externally, depending on the severity of the fraud. While this may work well for smaller organizations where decision making is taken by the CEO and a small group of senior management, it can pose a challenge for large organizations.

Figure 12: What action is generally taken in your organization upon the detection of possible fraud?



Large organizations often tend to have internal teams that may have limited capability to detect and unearth the fraud schemes. For instance, in our experience, technology based frauds often require specialist tools for investigation that large organizations don't tend to invest in. In such a situation third parties are often approached only upon the failure of internal teams/their lack of confidence to detect fraud. The time lost in making this decision (to hire experts) can significantly impact the time taken to detect fraud and recover losses. Smart fraudsters may use this time to cover their tracks, leaving the evidence trail cold.

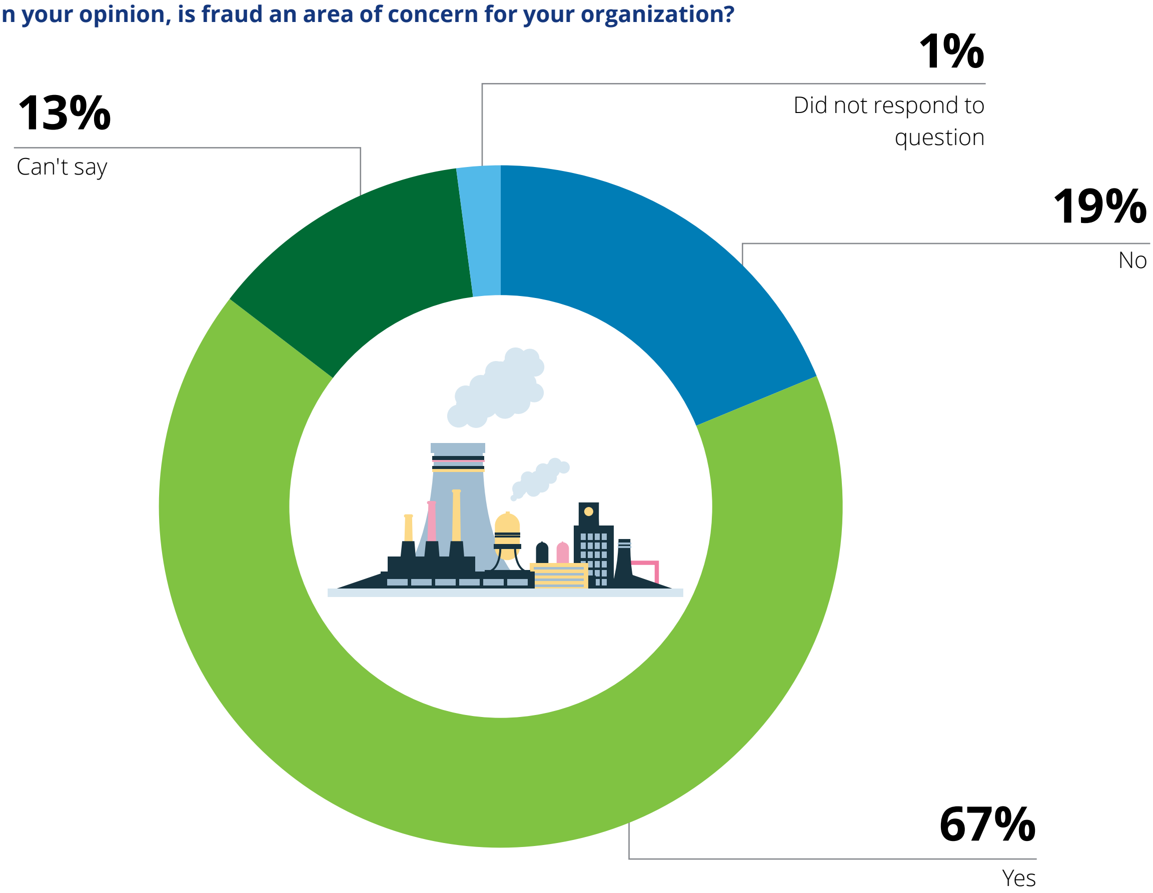
In dealing with the fraudster, responses elicited two diametrically opposite reactions: allowing the fraudster to resign in lieu of filing a legal case (36%) and taking legal action (32%). In our experience, we have also observed some leading organizations black listing such candidates and sharing the list of black listed candidates among their peers to prevent re-employment within the industry.

Focused on growth, the commitment to fight fraud is found wanting among small and medium companies

Bribery and corruption is a key concern

A majority of all businesses registered in India are small and medium enterprises. Of this, a significant proportion of companies are mandated by the Companies Act, 2013 to follow provisions pertaining to fraud prevention, detection and response. Given this strong focus on anti-fraud measures from regulators and law enforcement agencies, and in light of the efforts taken by larger corporates to prevent fraud, small companies can face tremendous pressure to view fraud seriously and take appropriate measures to tackle it.

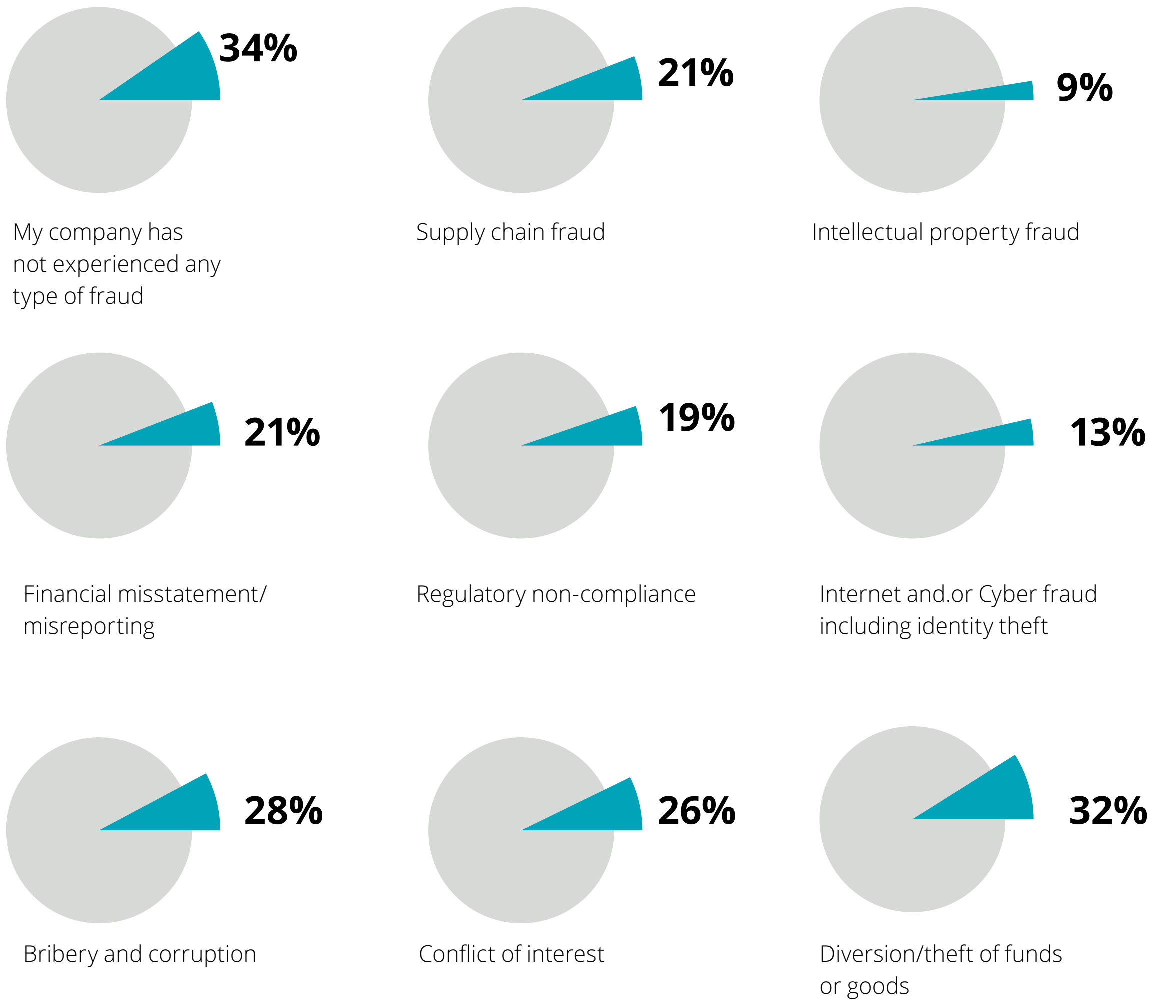
Figure 13: In your opinion, is fraud an area of concern for your organization?



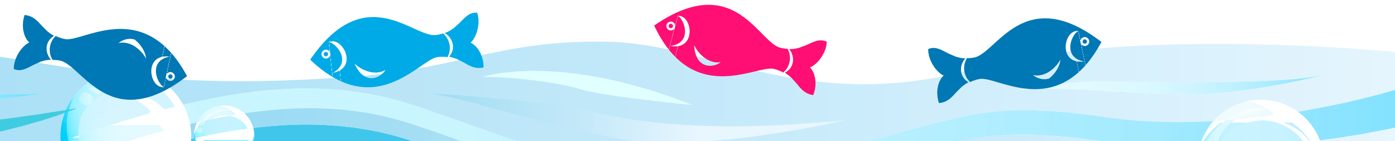
Around 67% of survey respondents said fraud was a concern for them and 54% believed fraud would rise in India over the next two years. Diminishing ethical values, limited/ lack of segregation of duties, and limited employee education on fraud were identified as the key factors that contributed to fraud.

When asked if their organizations had experienced fraud, the majority of respondents said 'no'. In our experience, organizations are unlikely to identify fraud if they don't have the right processes and systems in place. Specifically, in the case of small businesses, it is also possible that promoters/senior management may conduct business on a largely trust based model, relying on key employees to handle certain tasks. This can reduce the oversight they may have on all aspects of the business.

Figure 14: Which of the following types of fraud/misconduct/malpractice has your organization experienced in the last two years?



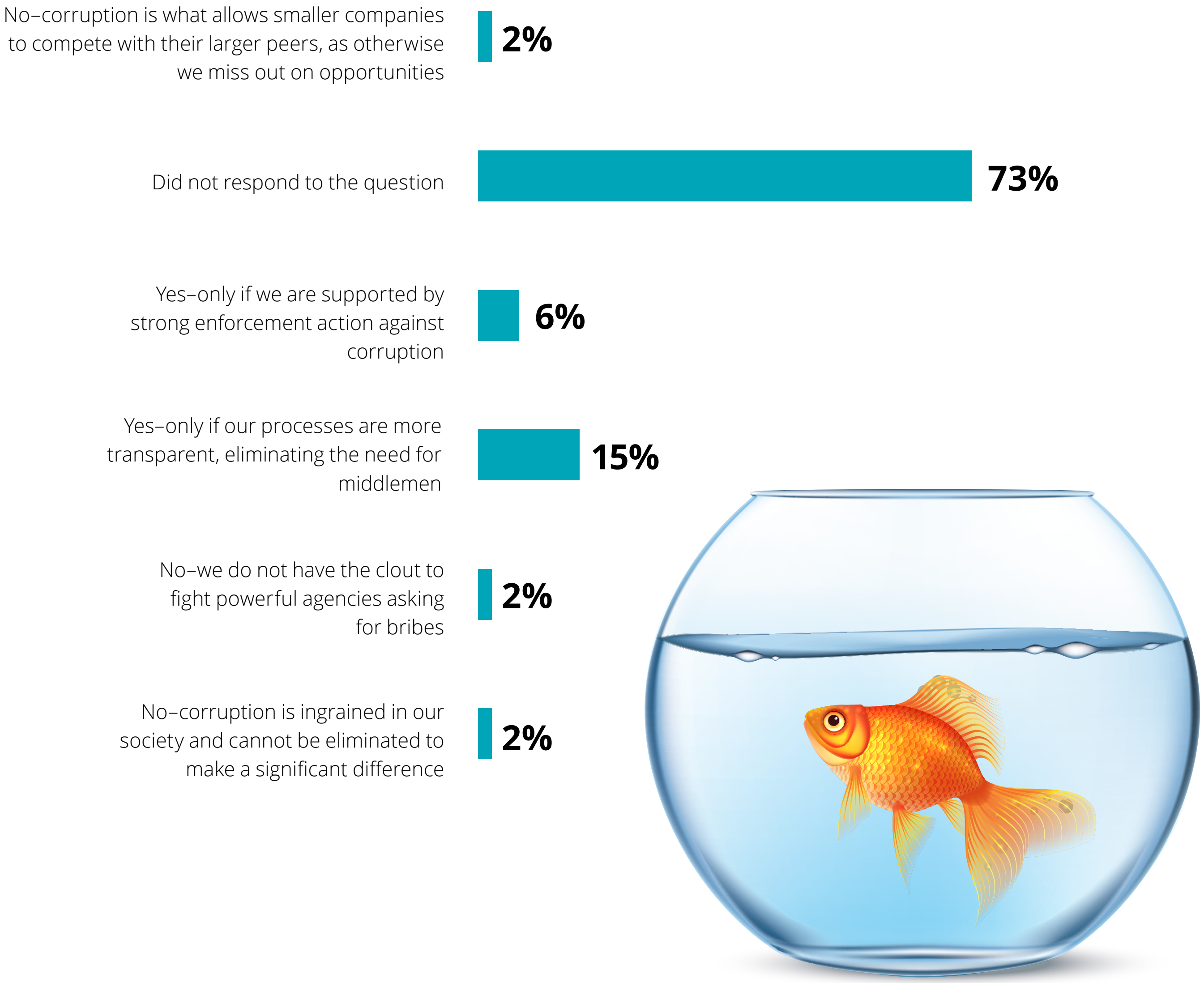
Note: This is a multiple choice question and responses will not add up to 100%



Among those respondents who mentioned their organizations may have experienced fraud, diversion/theft of funds/goods, bribery and corruption and conflict of interest were identified as the top frauds. Procurement (44%), and sales and distribution (29%) were identified as the top two processes vulnerable to fraud. Only 45% of respondents were able to quantify losses due to fraud, with 27% indicating they lost less than 1% of revenues and 8% saying they lost over 5% of revenues.

A significant proportion of respondents indicated experiencing bribery and corruption. Within corruption, collusive bribery (kickbacks) (69%), facilitation payments (69%), and commissions to third parties and agents (46%) were identified as the most common types of corruption faced. When asked if small and medium companies could conduct business in India without falling prey to corruption, the majority of respondents (73%) chose not to answer. Only 15% of respondents felt otherwise, provided processes (from the government side or with other business partners) were more transparent and eliminated the need for middle men.

Figure 15: Do you think small and medium businesses can conduct business in India without falling prey to corruption?

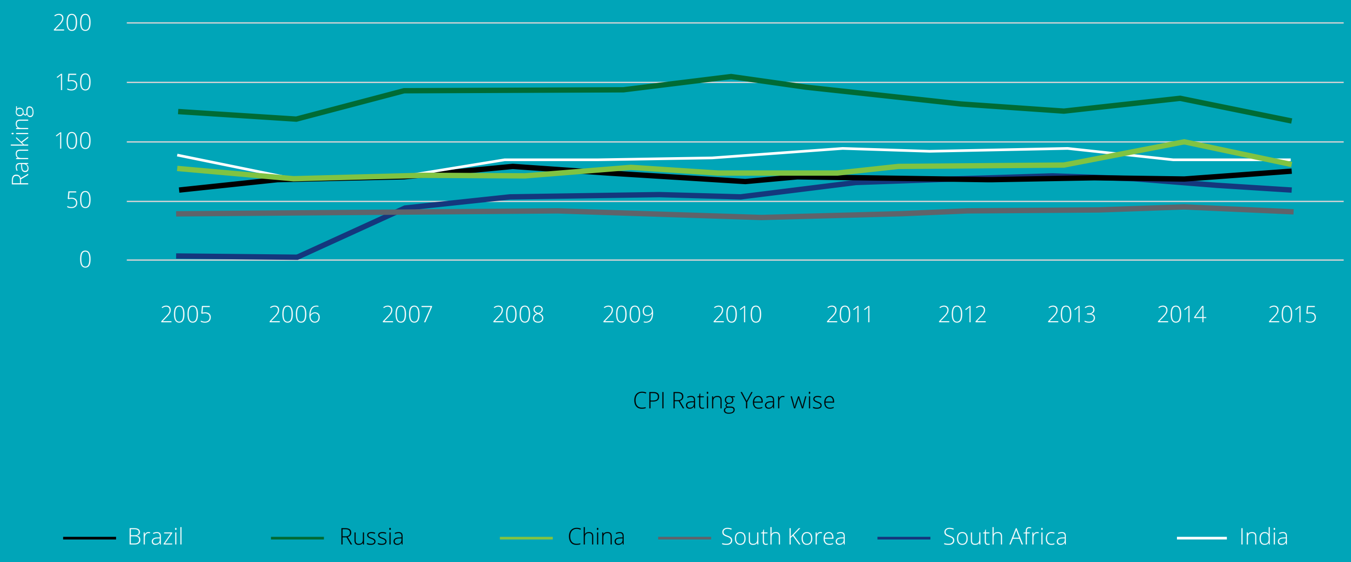


Point of View: Small and medium businesses need systematic intervention by the government to help tackle bribery

One of the reasons for the proliferation of bribery in India is the complex structure – comprising legal, tax and other frameworks - one has to adopt to conduct business. Small and medium businesses (SMBs) often don't have the capability and the resources to understand some of these frameworks (particularly those pertaining to anti-bribery and corruption) and deal with the inefficiencies and bureaucracy in government departments. To cope, SMBs tend to 'work around' these requirements, adopting practices that may be perceived as corrupt.

Corruption, however, is not a new phenomenon and neither is it a developing world problem, as recent unearthing of global fraud and bribery scandals may indicate. Yet some countries are perceived as less corrupt than others. It is hard to determine what these perceptions can be attributed to: major legislative changes, greater rate of prosecutions, higher fines, political shifts, public awareness schemes and other initiatives. But one thing is certain - while incidents of fraud can besmirch a country's image, systematic intervention by countries (among other factors) can help improve perceived corruption levels (as per rankings on the global Corruption Perception Index (CPI)). The chart below explains this.

Impact of government measures to tackle corruption



Our analysis indicates that CPI rankings have improved where governments have demonstrated action to curb corruption such as enforcing key legislation, adopting global best practices and commissioning third parties to develop white papers on the state of corruption. But rankings also tend to take a hit due to incidents of large scale fraud and corruption, nullifying the positive effect government action may have had.

For instance, in 2014, Brazil enacted the Clean Company Bill which set out a legal framework for making direct and indirect acts of bribery or attempted bribery of Brazilian public officials or foreign public officials illegal[9]. This appears to have contributed to a rise in CPI ranking from 72 in 2013 to 69 in 2014. However, the improvement didn't last long and a large scale scandal in 2014 involving a multinational oil company and several top government officials, impacted rankings that fell to 76 in 2015[10].

Since the occurrence of scandals and fraud cannot be controlled, it becomes even more important for governments to regularly demonstrate action to curb corruption so as to improve perceptions. In this regard, India has a long way to go.

India's path on the CPI over the last 10 years has been a turbulent one. In 2006 India was ranked 70, its best on the index in the last ten years. This was a considerable jump from 2005 where India was ranked 88th. While it's hard to pinpoint what events should be credited for this improvement, the impact of the Right to Information Act cannot be denied.

However, this positivity was short-lived with the ranking taking a major hit in 2008 (India fell to the 85th place) with the food riots[11]. The rankings continued to plummet between 2008 and 2011, as several scams unravelled. In 2011, India hit its 10 year low on the CPI at the 95th rank. Although India's CPI ranking during 2016 improved (to 76 from 84 in 2014), however the problem still persists as the CPI score remained same (38 in 2016 and 2015).

To tackle the graft, there have been several initiatives taken by the government including the following:

- Portal for Public Grievances launched (2007)
- CVC initiated National Anti-Corruption Strategy (2010)
- Introduced a biometric ID programme named Aadhaar with an objective to cut through the intermediary layers and allocate resources judiciously (2010)
- Ministry of Finance released white paper on Black Money (2012)
- New Companies Act and Jan Lokpal Act (2013)
- Prevention of Corruption (Amendment) Bill, 2013
- The Undisclosed Foreign Income and Assets (Imposition of Tax) Bill (2015)
- Right to information Act (2015)
- Launching digital India program and opening bank accounts to transfer subsidies for legitimate people (2015)
- Holding e-auction for transparent procurements (2015)
- Phasing out the use of ₹500 and ₹1,000 currency notes in return for limited quantities of new ₹500 and ₹2,000 notes being issued (2016)

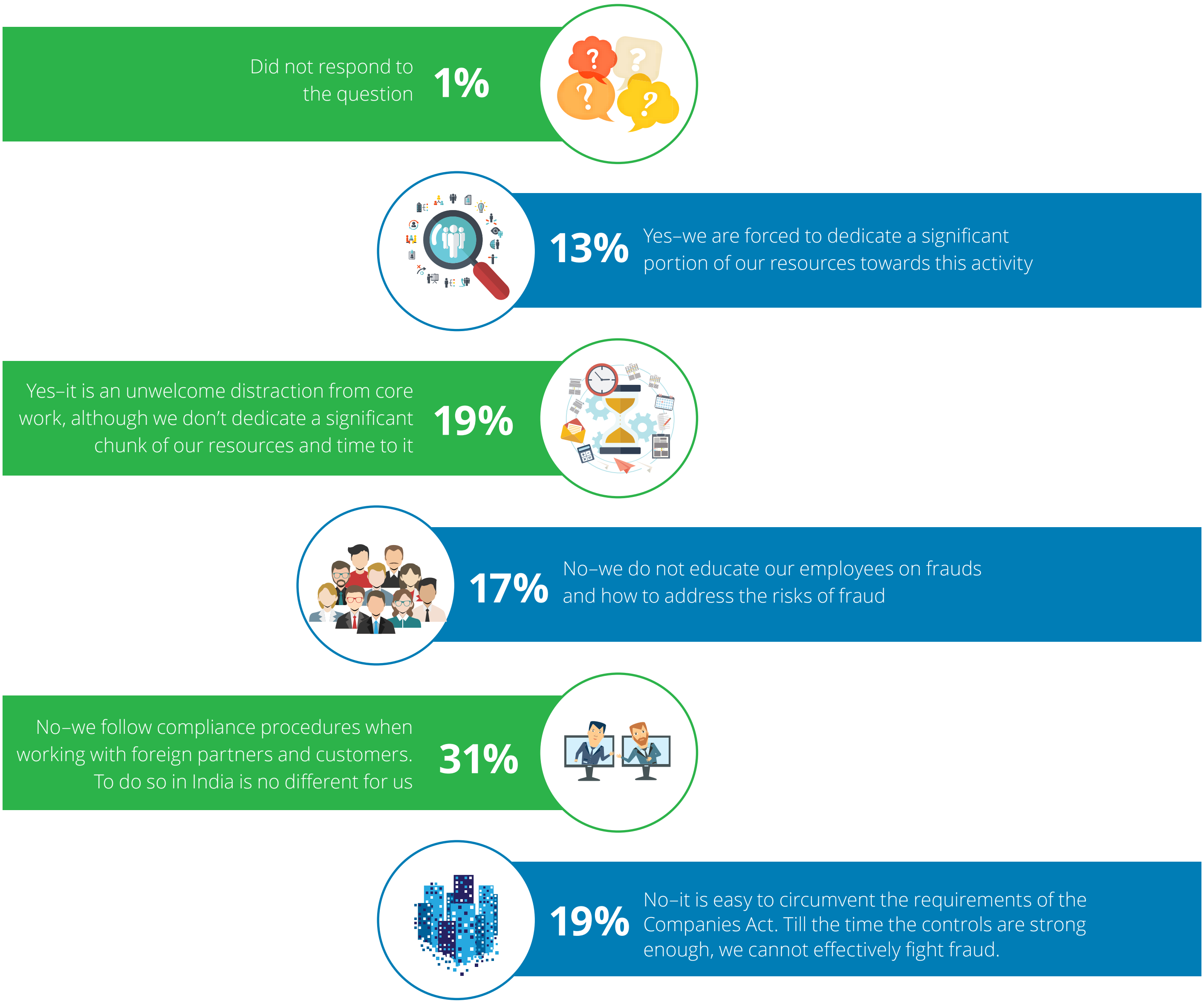
While these government initiatives appear to be in the right direction towards combating corruption, the effectiveness of these initiatives depends on the timely and efficient implementation by the government agencies. Fortunately, some of these measures have simplified procedures required to conduct business in India, and our ranking in the World Bank's **Doing Business** report 2016 is now 130–four places up from two years ago[12].

Alongside the measures taken so far, it is recommended that the government push for digitization in all spheres of business interactions, improving transparency around business processes and reducing the dependency on middle men and agents who are prone to corrupt activities.

[9] Source: http://www.jonesday.com/files/Publication/3c9b0192-a812-4849-b9fb-96fc1e520f70/Presentation/PublicationAttachment/ec9bf444-80c0-4892-af4a-9731b3d3c57c/Brazil%20Clean%20Company%20Law.pdf
[10] Source: http://www.telesurtv.net/english/analysis/What-You-Need-to-Know-About-Brazils-Petrobras-Scandal-20160313-0012.html
[11] http://in.reuters.com/article/idINIndia-29970920071012
[12] Source- http://indianexpress.com/article/business/economy/india-ranks-130-in-ease-of-doing-business-jumps-12-places-world-bank-report/

On working towards complying with anti-fraud clauses in the Companies Act, 2013, and other such regulations, the majority of respondents indicated that it may be a burden on them, with some respondents even indicating that the clauses could be circumvented easily. Around 19% of respondents felt compliance requirements were an unwelcome distraction from core work and 13% felt it forced them to dedicate a significant portion of resources towards compliance activities. Around 17% indicated they did not educate employees on fraud.

Figure 16: Do you think complying with anti-fraud clauses in regulations such as the Companies Act, 2013, places unreasonable burden on small and medium companies?



Did not respond to the question 1%

13% Yes–we are forced to dedicate a significant portion of our resources towards this activity

Yes–it is an unwelcome distraction from core work, although we don't dedicate a significant chunk of our resources and time to it 19%

17% No–we do not educate our employees on frauds and how to address the risks of fraud

No–we follow compliance procedures when working with foreign partners and customers. To do so in India is no different for us 31%

19% No–it is easy to circumvent the requirements of the Companies Act. Till the time the controls are strong enough, we cannot effectively fight fraud.

We believe compliance needs to be viewed as an investment and not a cost for organizations to benefit from it. This change of perspective is possible only if organizations see compliance as aiding them in 'doing the right thing for the right reasons'. Instead of a list of Do-'s and Don't-'s, compliance should be viewed as improvements to the organization that are tied to concreate outcomes such as better quality of deliverables, improved customer trust and business growth. Considering 31% of respondents have indicated that they are compliant with regulations while working with foreign customers/partners, it may be a matter of time before the same efforts can be extended for complying with Indian laws.

Lack of commitment impacts fraud prevention, detection and response initiatives

When asked if organizations felt they were adequately prepared to tackle fraud, 42% indicated in the negative. Further, 48% also citied lack of commitment as the primary reason for poor preparedness. In line with this, the key measures taken towards preventing fraud include using independent auditors to conduct periodic audits, implementing a code of conduct, regular manual monitoring, and assessment of fraud risks. It is no surprise that awareness creation features low on the priority list.

Figure 17: In your opinion, do you think there is enough commitment from small and medium businesses to address fraud?

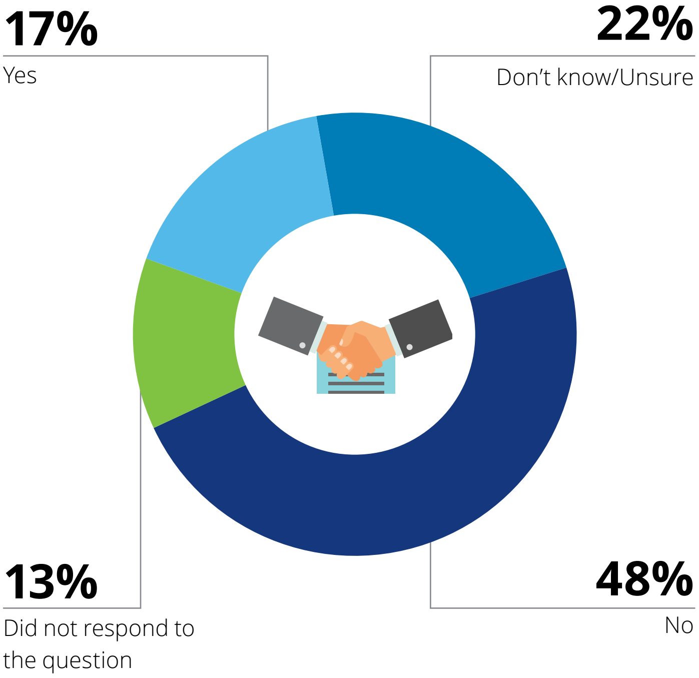


Figure 18: Do you believe your organization has allocated adequate budget and resources to deal with fraud related risks?

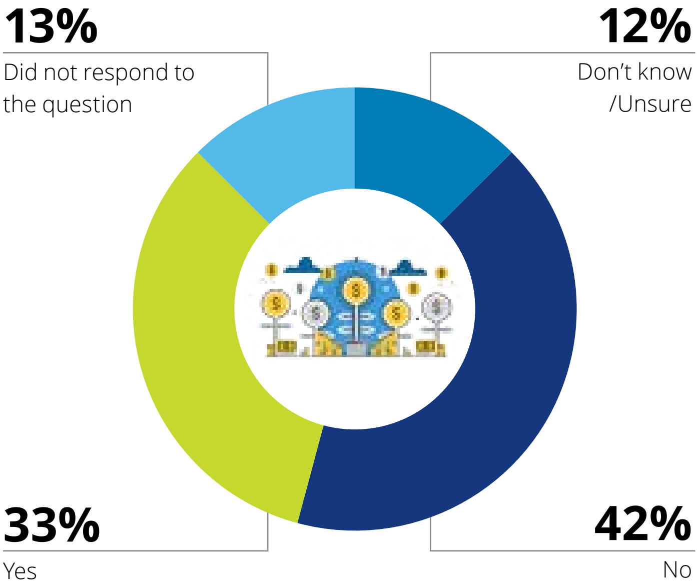
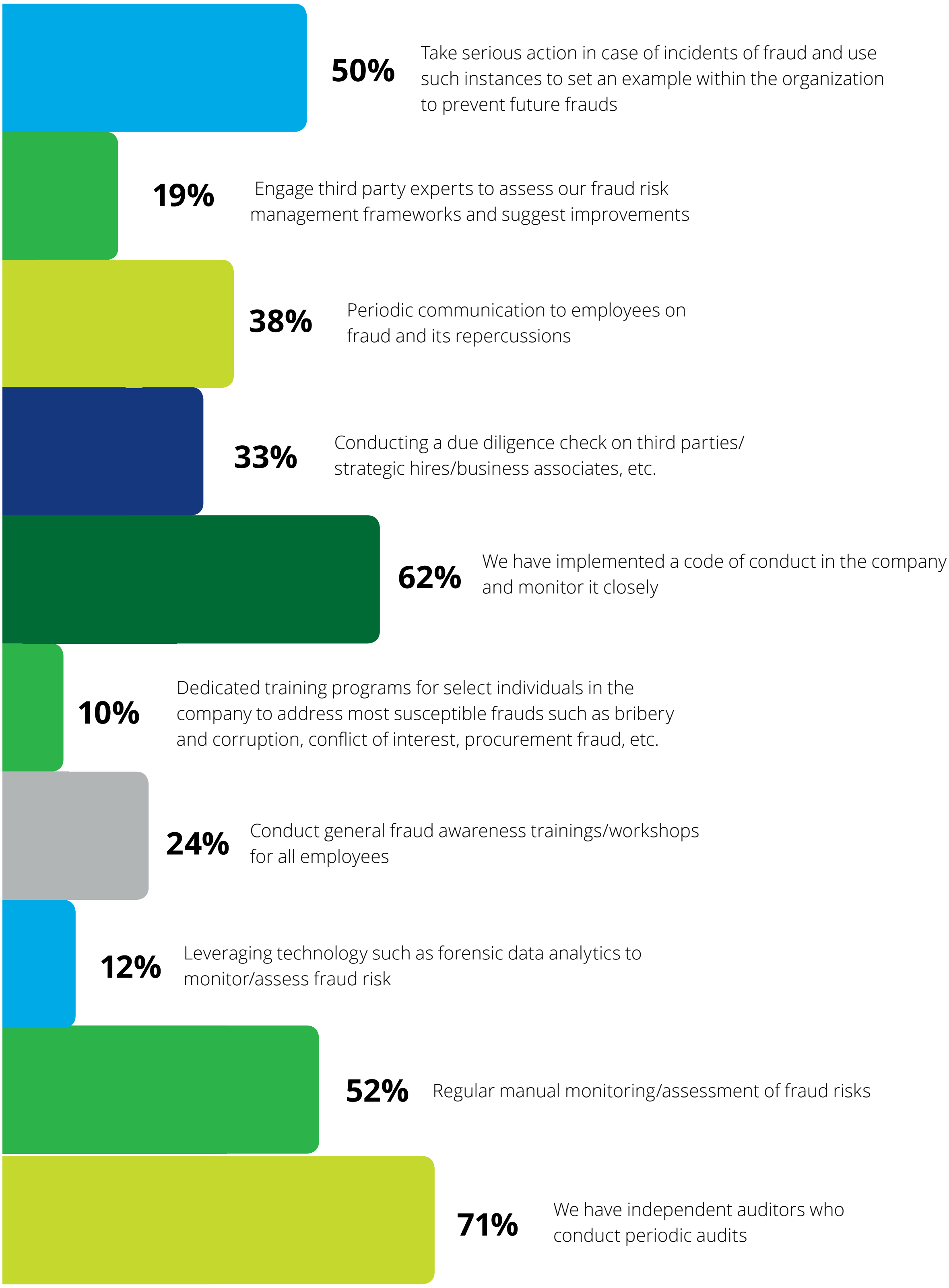
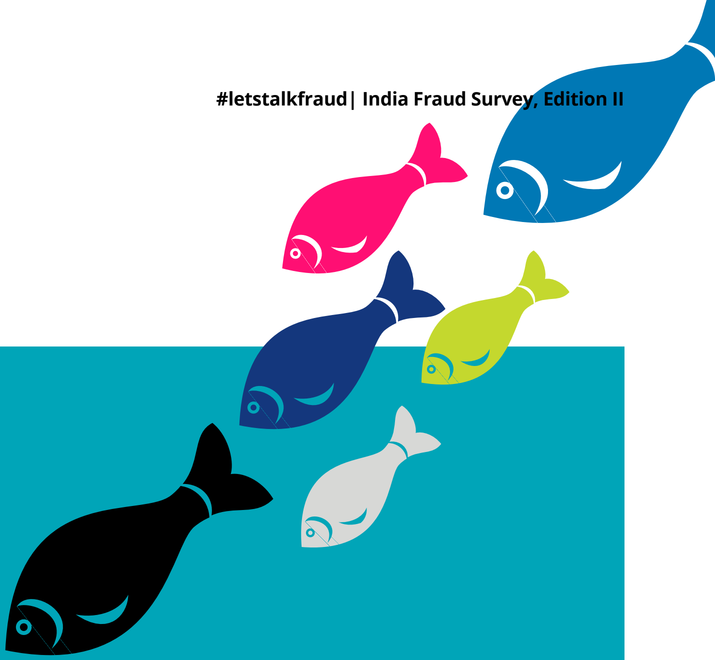


Figure 19: What action is generally taken in your organization to prevent fraud?



Note: This is a multiple choice question and responses will not add up to 100%



Point of View: Anti-fraud compliance programs can make a significant difference to fraud risk management efforts

Although fraud impacts all organizations alike, the repercussions of fraud in case of small businesses can be far more devastating than what is felt by large organizations. For starters, small organizations run the risk of losing key customers who may contribute significantly to their operations. Further, the cost of managing reputational damage and legal proceedings can be extremely detrimental to the future of the company. To successfully mitigate the impact of fraud, it is necessary for small businesses to invest in building an anti-fraud compliance program. Such a program should include anti-fraud policies and procedures, reporting mechanisms, training on these policies and procedures, and regular awareness creation efforts. Unless a company propagates its policies and procedures, by talking about them to employees and third parties continually, these measures will languish as mere documentation in some file cabinet.

Most organizations have some form of internal controls. However, against the backdrop of scandals and an increasing move towards greater transparency, law-makers are changing the regulatory landscape. The Companies Act, 2013, for instance, states several anti-fraud measures such as statutory audit, internal audit, whistleblowing mechanism, due diligence and awareness creation. Given this change, it is important to ensure that internal controls are reviewed regularly and necessary changes made to reflect current business realities.

Traditionally, the importance of anti-fraud compliance programs has taken a back seat at small businesses in their efforts to focus on growth and customer acquisition. However, recent incidents of fraud have prompted regulators to view the absence of formal anti-fraud compliance programs as akin to noncompliance, resulting in larger fines/ penalties for incidents of misconduct. Recently, a large corporation was pardoned for indulging in corrupt practices after it was able to demonstrate that the incident was a one-off, supported by evidence on a robust anti-fraud compliance program, including regular employee trainings on anti-bribery and corruption. In a landmark judgement, the company was not fined for its violation of the anti-bribery act[13].

Besides helping organizations comply with regulatory requirements, anti-fraud trainings have also shown to have a direct impact on the ability to detect and respond to fraud early, consequently losing much less (financially) to fraud. According to the Association of Certified Fraud Examiners (ACFE) Report to the Nations on Occupational Fraud and Abuse, 2016, companies with anti-fraud training programs were able to detect fraud 40% sooner and lost 50% less to fraud than companies that didn't focus on training.

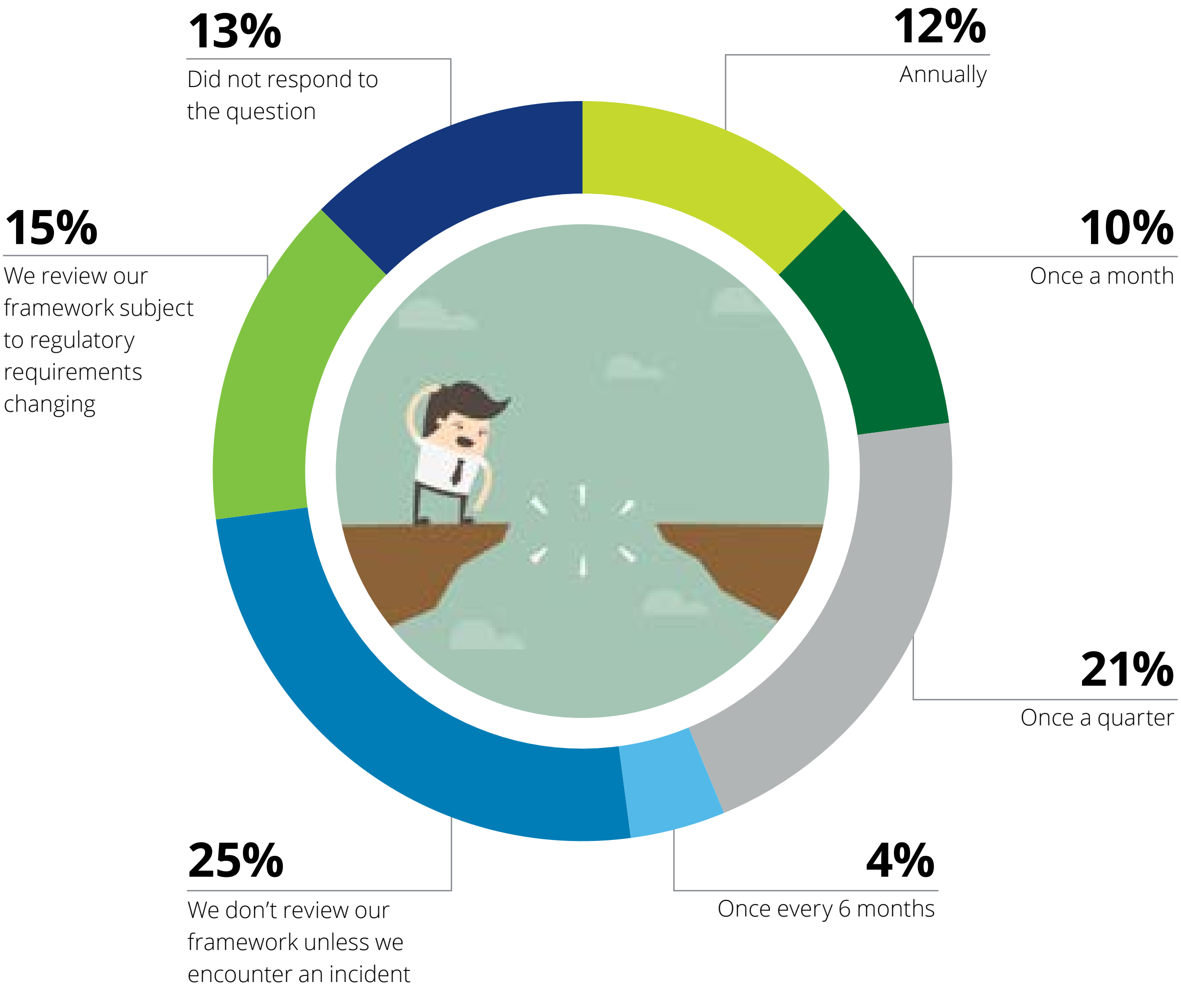
Lastly, anti-fraud training programs also present an opportunity for organizations to communicate their values – of ethics, integrity and fair practices – to employees, thereby improving employee morale and reducing attrition.

Small businesses wanting to invest in training programs today have several options, including web based e-learning solutions that cost significantly lower than class room based sessions, while providing flexibility to employees to complete the training when convenient. Leading e-learning providers today can provide in-built trackers, auto-generated reminders and completion statistics that can be shared with the senior management/ regulators etc. as documented evidence of anti-fraud efforts.

[13] Source: http://www.jdsupra.com/legalnews/landmark-sec-decision-cites-compliance-65138/

Review of controls to prevent fraud appeared to be undertaken irregularly with 40% of respondents stating they waited for external triggers (either an incident or regulatory change) before reviewing their internal controls.

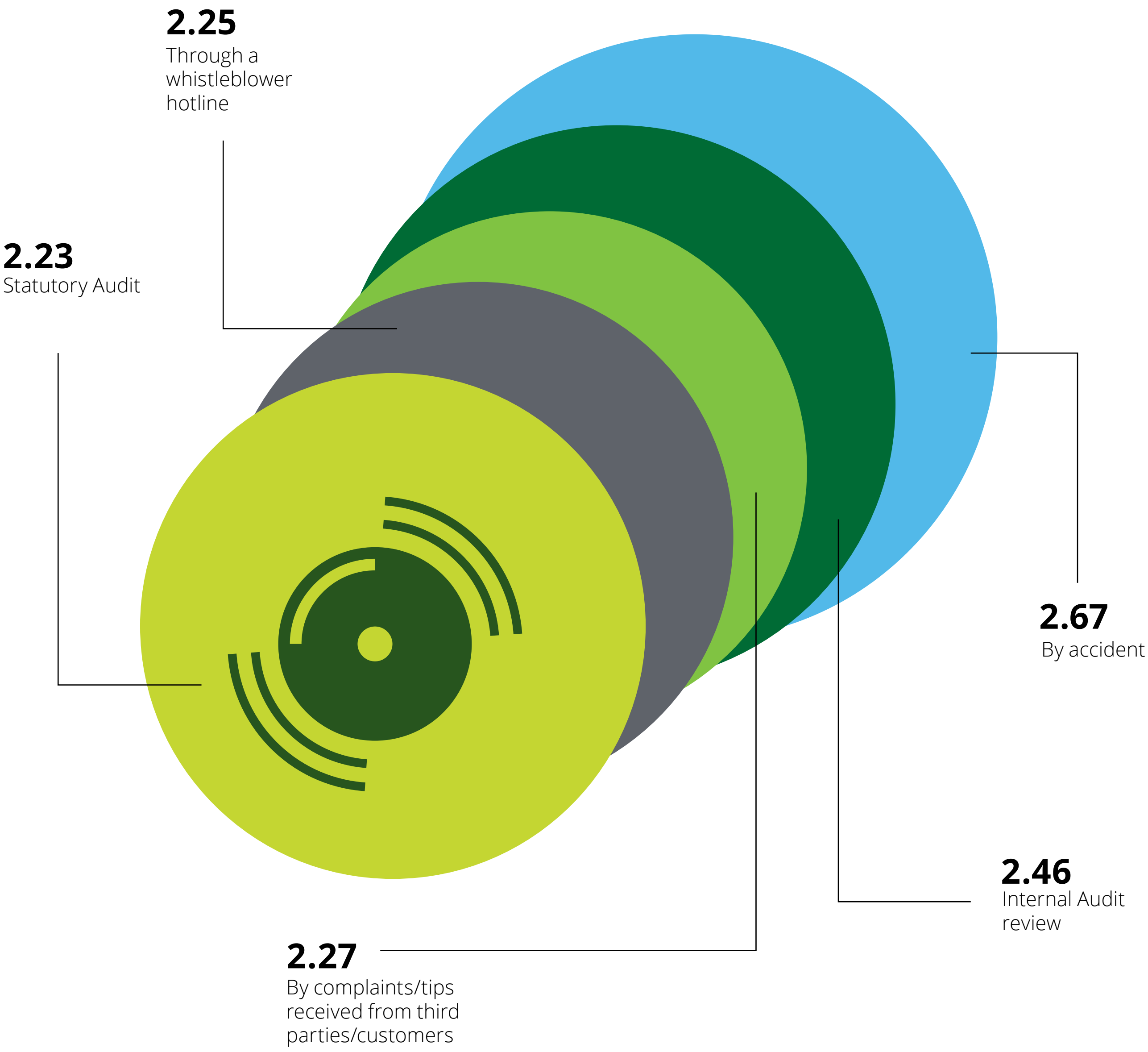
Figure 20: How often do you review your fraud risk management measures?



Further, 58% of respondents said fraud related observations were addressed immediately from the time they were reported. Around 23% of respondents said they were addressed within one-two months from the time they were reported. In our experience, fraudsters are usually ahead of the curve and to prevent fraud or detect it in its initial stages, it is important to regularly review and update internal controls. Also, organizations should not ignore any outliers, be it with respect to data or processes.

In the area of fraud detection, organizations appeared to rely on internal audit, complaints and tip offs from customers, and accidental detection of fraud. While many small organizations may not be required to have an extensive vigil mechanism under the Companies Act, 2013, it is important to rely on multiple channels to detect fraud. Some of these include instituting a statutory audit that focuses on identifying irregularities/ noncompliance as part of ascertaining the accuracy of the organization's financial records, relying on surprise audits (again by internal or statutory auditors), and job rotation for employees in key functions.

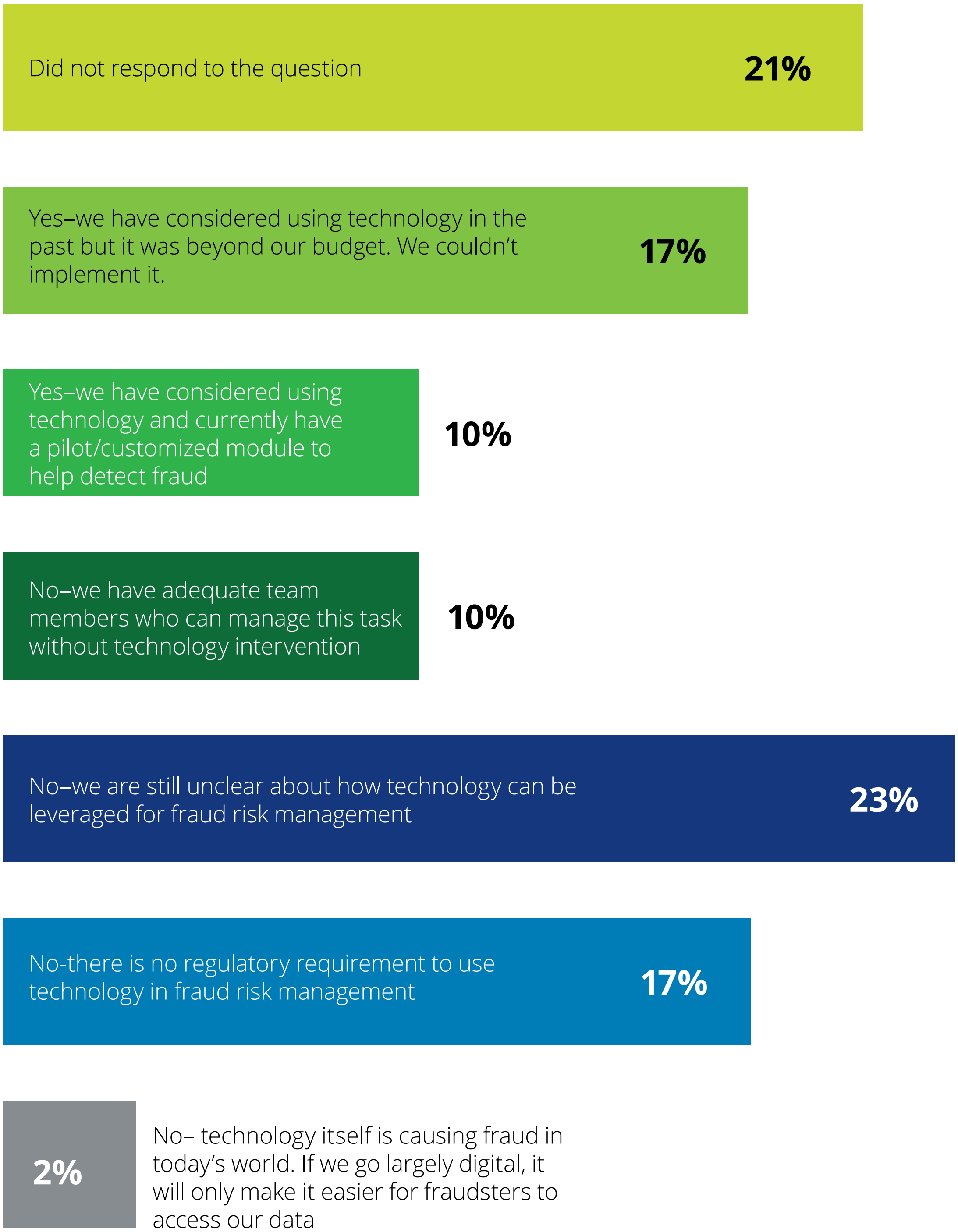
Figure 21: How are fraud incidents detected in your organization?



Note: This is a multiple choice question and units shown are the weighted average of responses

When asked if small and medium enterprises considered leveraging technology to detect fraud, only 27% of respondents confirmed.

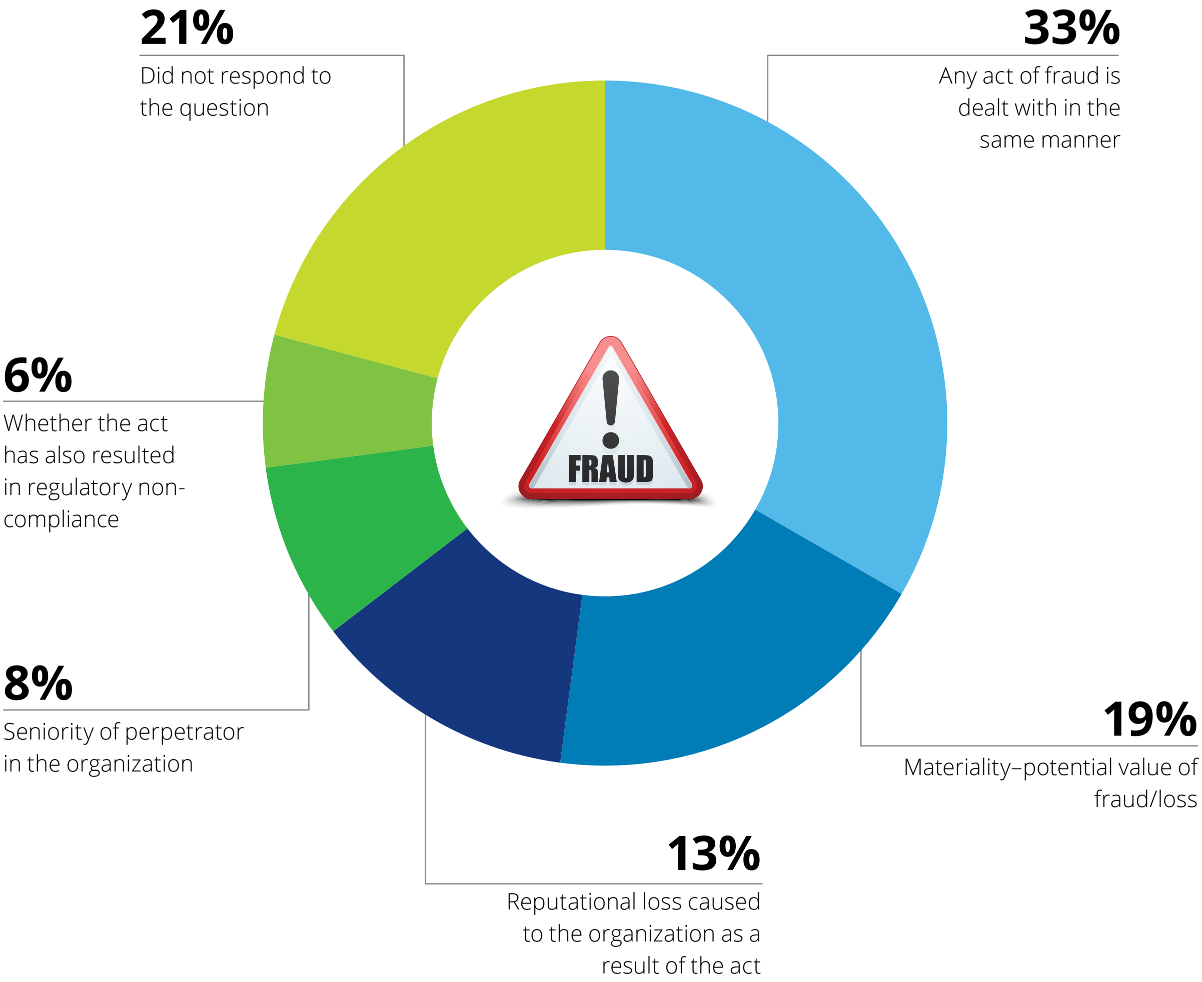
Figure 22: Have you considered leveraging technology to help your organization tackle the risk of fraud better?



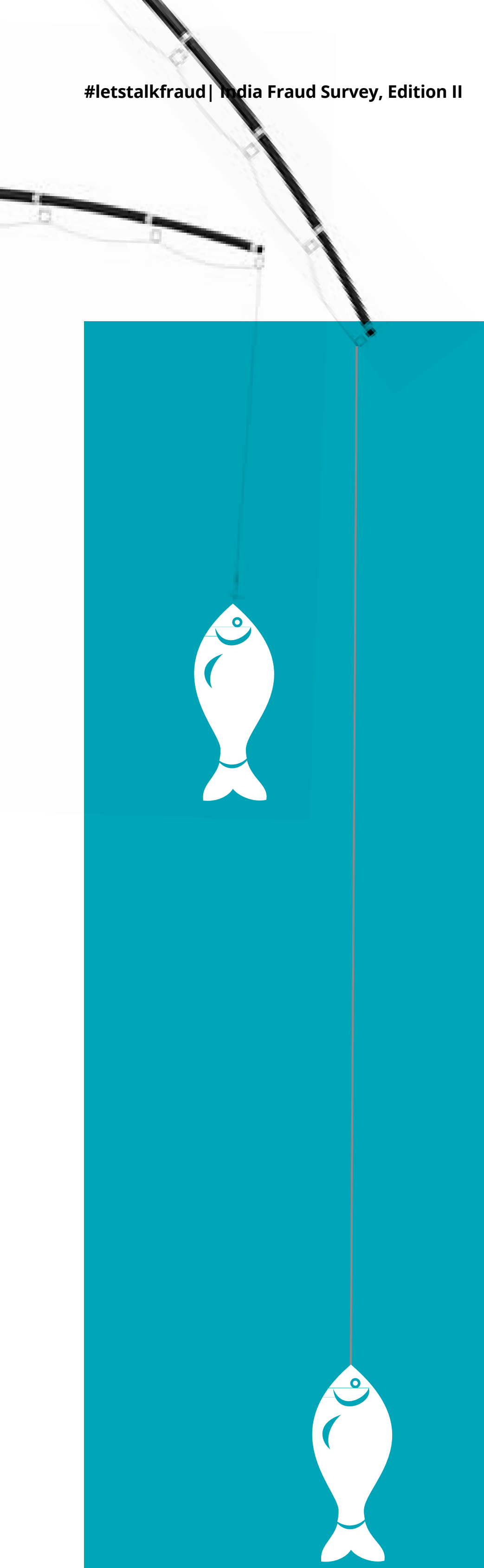
Upon the detection of fraud, the majority of respondents (71%) said they internally investigated the issue. About 53% said they reviewed existing controls, and 53% said they asked the fraudster to resign.

Stringent action appears to be dependent on the materiality of fraud (19%), followed by whether the fraud also resulted in regulatory noncompliance (6%), involvement of senior employees (8%), and any obvious reputational loss (13%). Only 33% of respondents felt all frauds were dealt with in the same manner.

Figure 23: What factors drive a more stringent course of action in your organization upon identifying an instance of fraud?



In our view, it is difficult to estimate materiality of frauds as functions within organizations often work in silos. In the case of small businesses people tend to closely guard information and therefore the extent of misuse can be greater than what it appears.



Point of View: Kick-starting fraud risk management at small businesses

Small businesses are significantly more likely than their larger counterparts to neglect instituting basic anti-fraud controls that can save them from costly losses, as inferred by our survey responses.

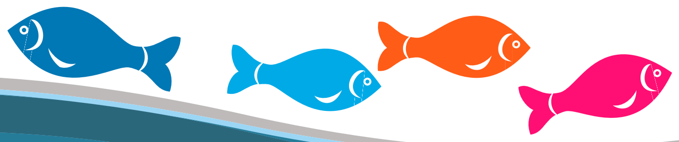
One of the common perceptions that small businesses tend to carry is that fraud risk management is a costly, time consuming activity, and hence best approached when the business reaches a certain critical size. This impression is also bolstered by the fact that the Companies Act, 2013 exempts small businesses from certain clauses pertaining to fraud risk management. However, in our experience, small businesses tend to lose more to fraud– monetarily (as a proportion of business revenues) as well as reputation wise- than large businesses. This makes it imperative for them to focus on building effective internal controls.

Small organizations can consider instituting the following measures as a start to their fraud risk management journey. These are neither expensive nor very time consuming[14].

Enhancing the scope of internal audit– Internal audits can help review accounting processes to validate financial information, discover any errors, test internal controls, and identify any gaps and limit the legal and tax related damages that the business may otherwise suffer.

Management certification of financial statements– This indicates that the business understands the observations made by the audit team (internal and external) pertaining to the organization's financial position, fraud risks, and any other concerns. It also signals a willingness on the part of the organization to address any concerns in the future.

[14] Compared to some of the traditional processes such as Finance, Operations and Sales that the business may invest in, as well as compared to the time and effort spent in fraud detection and response.



Division of responsibilities- There should not be abundant concentration of job responsibilities in key functions. For example, in the Purchase department, the requestor, negotiator, and approver should be different people. Also, there should be multiple signatories to authorize transactions above a certain threshold. In our experience, some of the functions susceptible to fraud include sales, procurement, cash and bank operations, and employee reimbursement claims process. This can be a starting point for small and medium businesses to initiate division of responsibilities.

Undertaking formal fraud risk assessment of key processes- Whether conducted by third party organizations or undertaken internally, fraud risk assessments of key processes and functions within an organization can help understand the level of fraud vulnerabilities better. If it is conducted internally, it should be conducted by personnel having in-depth knowledge of the business and market with knowledge and experience of fraud. Some of the suggested processes that should be regularly reviewed include Sale (order to cash) process, Procurement (procure to pay) process, Inventory management, Financial reporting and closing (record to report) process, cash and bank operations and employee expense reimbursement claims process.

Defining a code of conduct – A code of conduct which is tailored to the needs of the organisation and adequately covers anti-fraud clauses, can help set the tone among employees/third parties of ethical and unethical practices and penalties associated with undesirable behaviour.

A channel for employees/ third parties to report suspicions – While most small businesses tend to expect employees to report suspicious activity to their managers, it is also important to provide an independent channel – such as an unmanned complaint box, dedicated email ID, or installing a toll free number, that employees/ third parties may use to report such instances, without fearing retaliation.

In our experience, small businesses with robust corporate governance and fraud risk management practices tend to attract investment opportunities and advice that can help them grow.

Employees want to play an active role in fighting fraud - Perspectives from working professionals

Nobody likes to work for an organization perceived as fraudulent or indulging in unethical practices[15]. Just like organizations, employees too tend to suffer the consequences of fraud at the workplace– low morale, job uncertainty, social stigma and discrimination by prospective employers. Today, more than ever before, the role of employees in preventing fraud cannot be undermined. A majority of our survey respondents (56%) felt they were primarily responsible, as employees and citizens, to prevent fraud.

It is therefore disheartening to note that the majority of respondents (65%) also felt that corporate fraud would rise in the next two years. Respondents identified bribery and corruption, financial statement fraud, and embezzlement of funds as the top frauds that they suspected their organizations to have experienced.

[15] About 88% of survey respondents to Deloitte India survey report on Public Perception of Anti-Bribery and Corruption Compliance efforts, 2014, said they did not want to work for a company perceived to be indulging in corrupt practices.

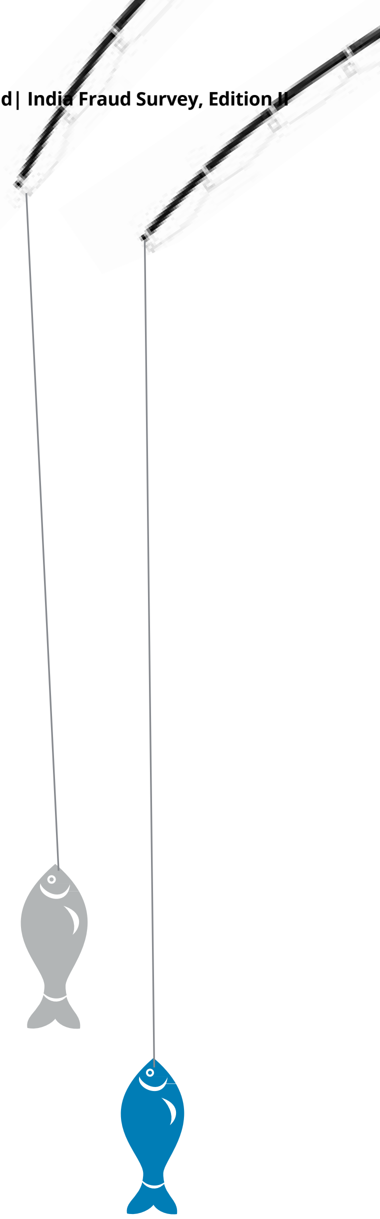
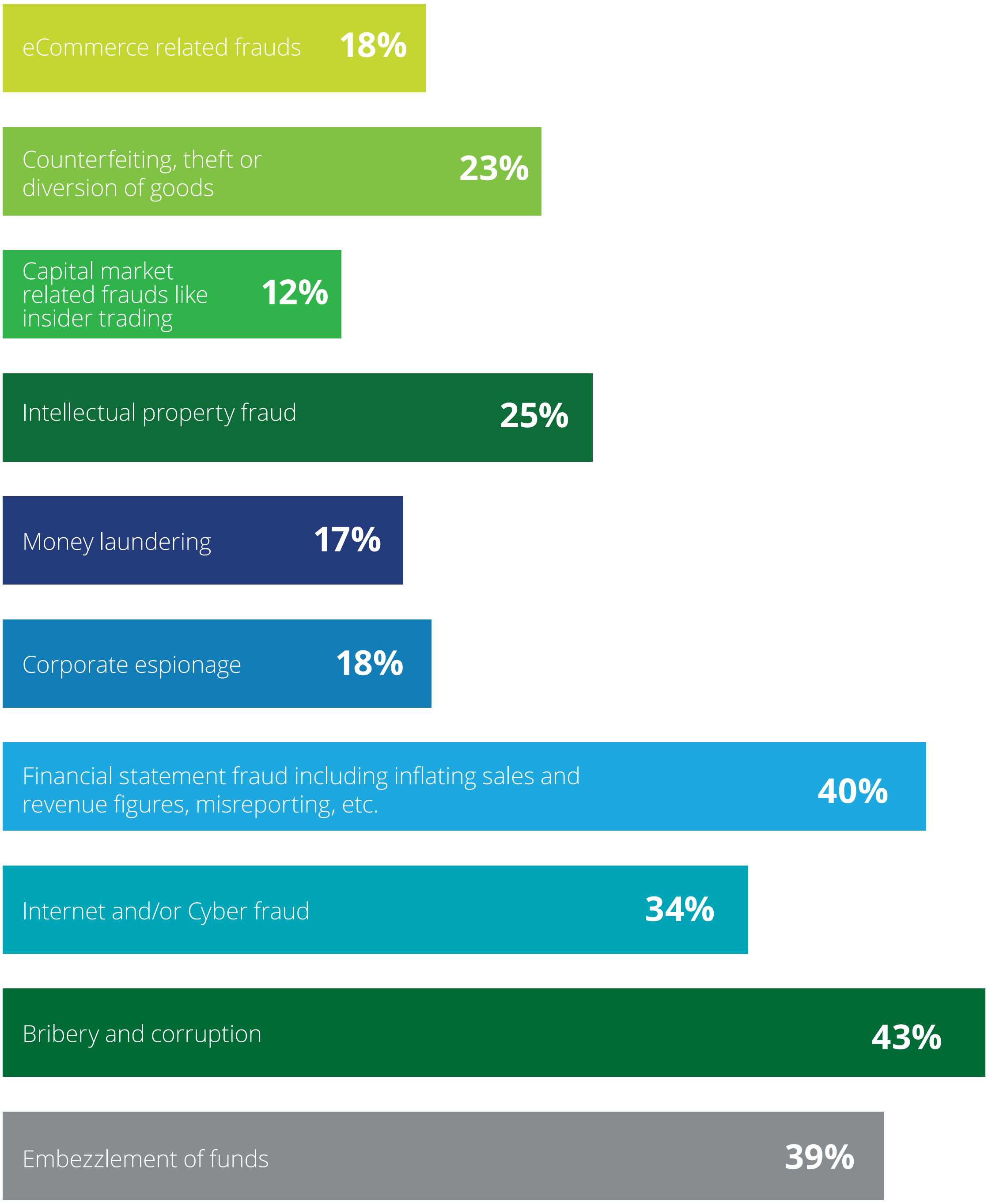


Figure 24: Which of the following types of fraud/misconduct/malpractice do you suspect your organization has experienced?

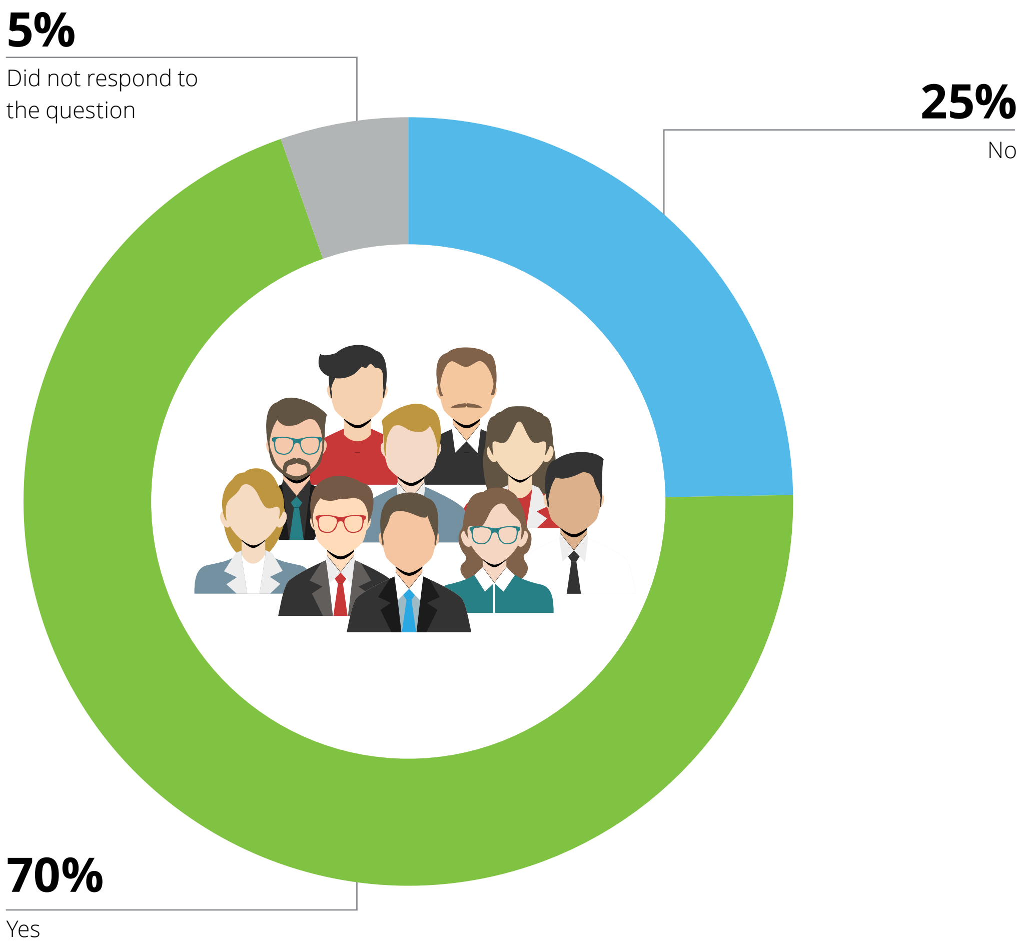


Note: This is a multiple choice question and responses will not add up to 100%

Weak/ ineffective controls (65%), technological advancements (46%), and a general decline in ethical values (42%) were identified as the top three reasons for the presence of fraud.

About 70% of respondents felt their organizations encouraged them to report suspicious activity pertaining to unethical behavior or fraud and 74% indicated they were unaware of malicious behavior towards whistleblowers.

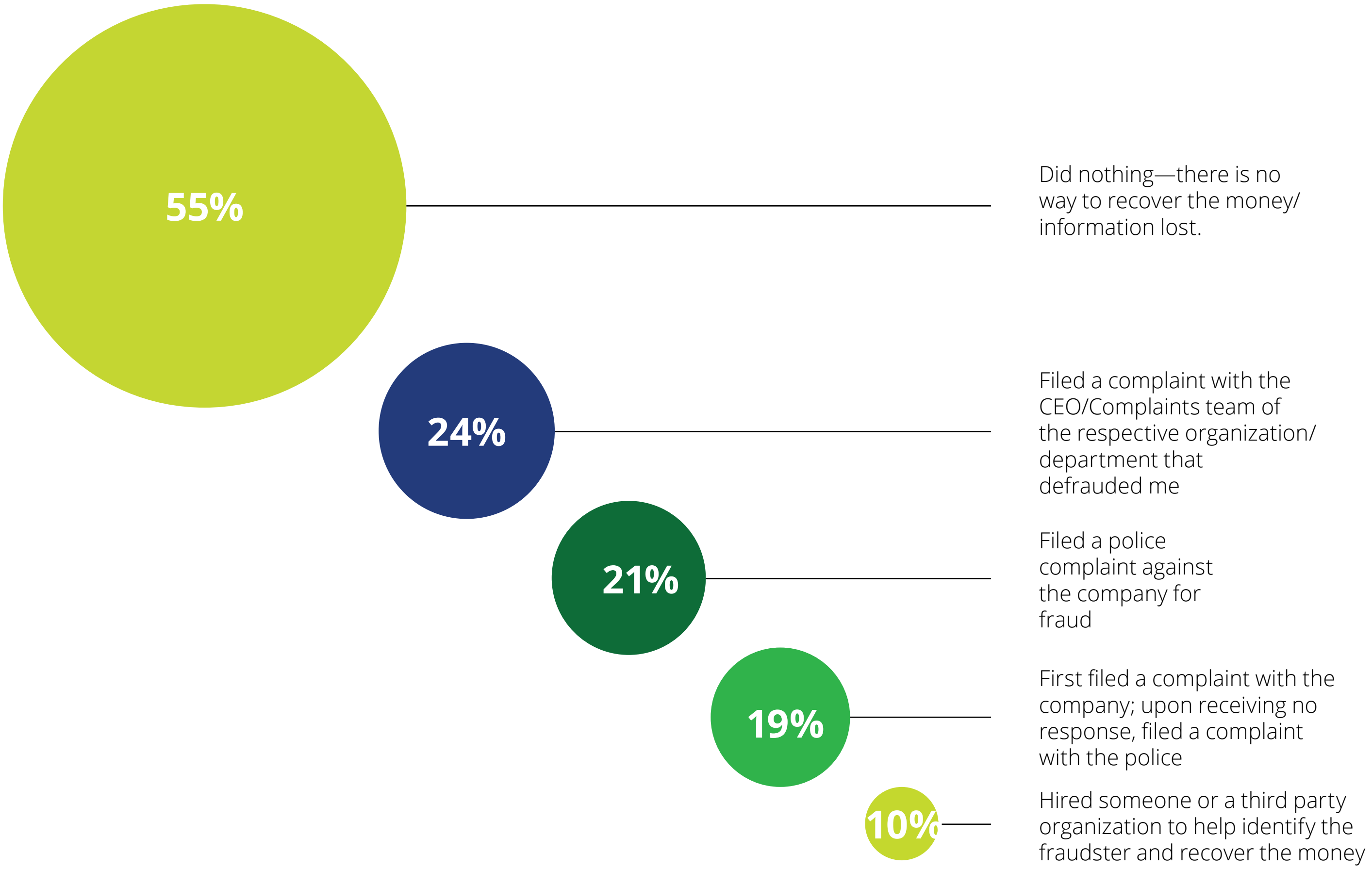
Figure 25 : Do you feel your employer provides enough opportunities to encourage employees to come forward with information related to unethical activities, without them having to fear the possibilities of retribution or deliberate victimization?



In our experience, one of the reasons for fraud to prevail is the tendency of organizations to keep fraud outside the purview of employees and/or taking token measures to involve them. It is heartening to note that this situation appears to be changing and employees are not only more aware of fraud but also encouraged to report it.

Interestingly, this behavior contrasts how working professionals deal with fraud in their personal lives. Among respondents who indicated they (or their families) had personally experienced fraud, the top fraud schemes included bribery and corruption at government offices, identity theft and specific frauds involving charities and/or loyalty points. About 44% of respondents said they had lost less than ₹1 Lakh, whereas 11% said they lost between ₹1 Lakh and ₹5 Lakh. Despite the scale of loss, the majority of respondents indicated that they took no action, as they felt recovery was not possible.

Figure 26: What actions did you take upon realizing you were defrauded?



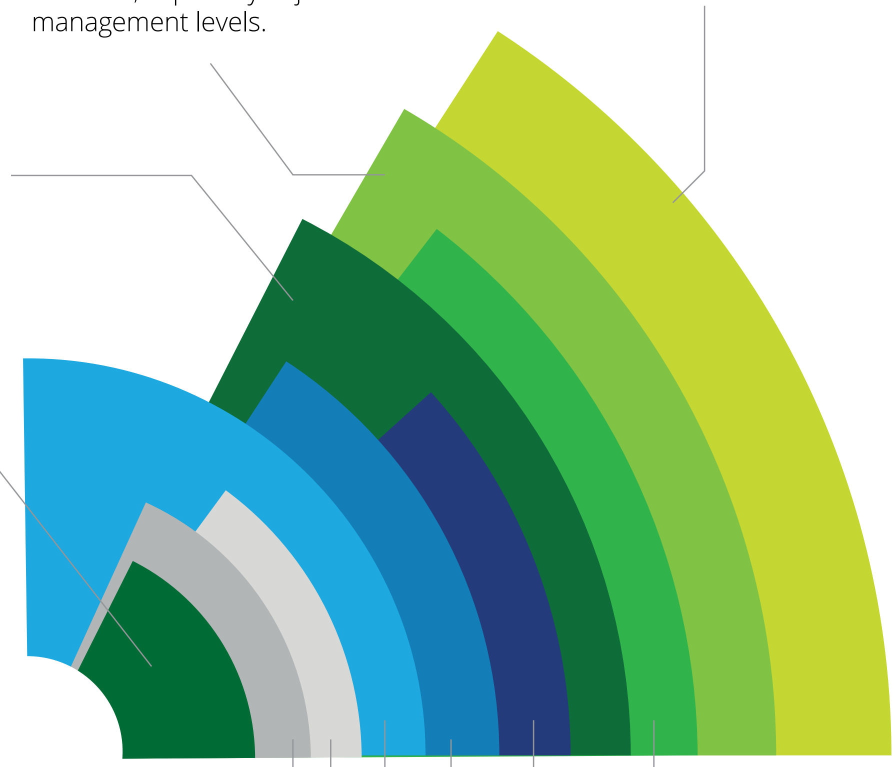
Note: This is a multiple choice question and responses will not add up to 100%

There was mixed reaction from respondents on the efficacy of Indian laws to prevent fraud with 47% saying the laws could be a strong deterrent only if they were enforced regularly and punishments were meted out frequently, and 42% saying laws (existing or otherwise) were a poor deterrent.

One can draw a similar parallel in the corporate environment, where inaction/ inadequate response towards potential fraud reported by employees may result in low employee confidence in the fraud reporting process, eventually leading to distrust of internal channels. Organizations therefore need to focus on ensuring that investigation and response to report suspicious activity is undertaken in a timely and efficient manner, and that these are communicated appropriately to employees.

Besides law enforcement, respondents felt that the following measures taken by corporates and the government would best help prevent fraud: Greater adoption of digital technology and regular advisory on known frauds (provided by the government), and open discussion on fraud and recognizing employees and rewarding them for ethical behavior (by corporates).

Figure 27: According to you, which of the following measures may help reduce fraud in India?



59%

Recognize employees (government and corporate) and reward them for demonstrating ethical behavior, especially at junior management levels.

57%

Name-and-shame wrong-doers.

63%

Greater adoption of digital technologies to reduce human interaction for routine tasks–both at corporate and government levels (e.g. eProcurement)

63%

The government should provide more information; for example, issue an advisory on key fraud schemes so that citizens can understand and prepare themselves to avoid such situations

52%

Educate police and better equip them to deal appropriately with fraud cases

61%

Corporates should talk more openly about fraud and educate their employees on how to safeguard themselves

57%

Government departments should discourage middlemen from transacting on behalf of individuals and promote more public-private partnerships (e.g., the passport office)

42%

Legalizing small off-the record payments made (like a Tatkal fee to reduce transaction time) for better efficiency

53%

Senior management should play a more active role and especially speak about mitigating fraud more often

90%

Stronger enforcement of laws in cases of fraud, including quicker judgements and harsher penalties

Note: This is a multiple choice question and responses will not add up to 100%

Point of View: Building a case for 'employee influencers' - Involving the individual in the fight to prevent corporate fraud

As the legal and regulatory landscape in India evolves, we are likely to see a rise in enforcement activity including hefty fines and possible business debarment/closure in response to fraud, misconduct and noncompliance. Organizations are not the only ones to feel the impact. Employees too tend to face social stigma and uncertain prospects in the job market due to their association with tainted companies. To manage this situation better, there is need for employee influence, wherein employees play an active role in combatting unethical behavior in order to safeguard their jobs and build organizational (and, through that, their own professional) reputation.

A global survey report has indicated that one out of every five employees is an 'employee influencer' who is deeply engaged with his/her employer(s)[16]. These employees defended their employers from criticism and acted as active advocates both online and offline. Such influential employees can also help cultivate a positive and ethical work environment within organizations. In addition to regular trainings, employee influencers can be groomed to become ethics advisors who increase awareness of company policies and help hold their peers and supervisors accountable; they can also be made part of dedicated committees to ensure programs promoting ethical behavior resonate within the organization.

Considering many of these employees already have a strong moral compass, the organization would need relatively less efforts to train and engage them to support its values in public.

To identify and cultivate employee influencers, organizations can consider the following measures:

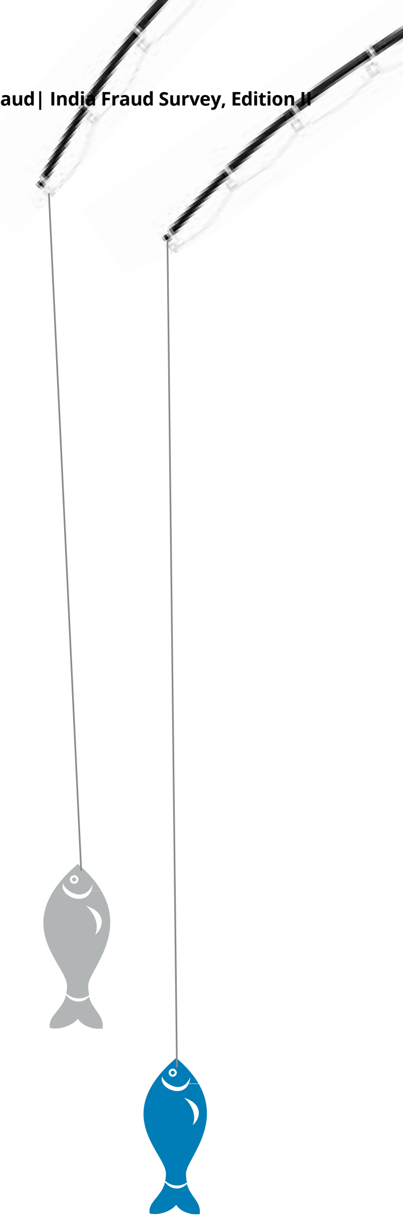
- **Create a culture of 360 degree feedback** where employees are encouraged to give feedback on their respective managers' actions, specifically any suspected unethical behavior or concerns around transparency. If this is perceived to be intimidating to the employee, organizations can look at designating a section of mid-to-senior people as feedback coaches, who are perceived as friendly and open to receiving feedback from employees and communicating it to the intended recipients.
- **Conducting employee surveys** to understand the sentiments around ethical behavior which can reveal several findings that can provide the grounds for developing action plans. They can also reveal candidates with a strong ethical quotient who may be considered for being employee activists.
- **Reward ethical behavior.** While this may sound counter-productive, in today's business environment it is imperative that organizations 'see' and 'read' about positive role models. This also gives the organization a chance to demonstrate its commitment to ethical values and employee activism.
- **Being approachable and explaining your actions** to employees is easier said than done. However, most organizations/ leaders gain trust and credibility only when they respond to employee feedback and demonstrate action taken. Even if no action was taken on a suggestion, it is important to explain 'why' to employees so that they continue to provide new ideas. Some measures taken by leader(s) to be perceived as approachable include relying on informal meetings, elevator conversation, and interactions over coffee or lunch. Some leaders also ask open ended questions to employees such as the following: "if you were in my place, what is the one thing you would change tomorrow?", "what makes you ashamed of our organization?", "what do clients say about our business?", "What more can we do to receive feedback from employees?", "how can we improve our ethical quotient as an organization?".

Investment wizard Warren Buffet once said, **"It takes 20 years to build a reputation and five minutes to ruin it."** In their fight against fraud, organizations have a very powerful ally in their employees. Employee influence needs to be encouraged.

Working professionals today are concerned about fraud. They are willing to be part of the solution to tackle fraud and safeguard the interests of their employers and society. Is the society/employer willing to give these anti-fraud influencers an active role?

[16] Source: Employees Rising: Seizing the Opportunity in Employee Activist, a survey by Weber Shandwick and KRC Research. https://www.webershandwick.com/uploads/news/files/employees-rising-seizing-the-opportunity-in-employee-activism.pdf

The future of fraud – Business developments that can impact the fraud landscape in India



India is perhaps one of the few countries in the world to nurture businesses of all types, sizes and maturity levels-from manpower intensive industries that are governed by decades-old laws to technology facilitated services that are relatively under regulated. Many organizations have business touch points across the spectrum of the Indian business landscape, making them perhaps more vulnerable to fraud risks, than organizations that work in a relatively homogenous business landscape, where policies and procedures may be fairly similar. This means that a fraud risk associated with one business touch point, if not managed properly, can quickly spread across the organization and disrupt functioning.

We believe this aspect will increasingly become a concern for organizations as they move towards embracing new technologies and business models. For instance, the adoption of blockchain technology in some organizations globally has resulted in significant changes to the way the security departments are structured. Technology that enables the Internet of Things (IoT) paradigm essentially links a manufacturing process (physical devices embedded with sensor) to a services business model (online decision making basis certain inputs), impacting the entire organization in the long term.

Have organizations thought about how such decisions to modernize may increase their vulnerability to fraud? What if the fraudster is also facilitated by technology to expand his/her sphere of attack?

This section comprises a series of point of view documents, developed on the basis of our experience in helping companies tackle fraud even as they attempt to embrace new business paradigms.

Blockchain - Can an alternate technology that aims to curb fraud gain credence?

Blockchain gained popularity about seven years ago, as the underlying platform powering Bitcoin, a popular virtual cryptocurrency. However, over the past year, several large corporations including many investment banks, have begun to test and work with blockchain technology, exploring its potential to reduce costs and improve efficiency of transactions.

Blockchain overcomes the traditional challenges of having a 'wall of security' around data that can (in theory) be breached by those having access to it such as administrators. Often such access can be misused by individuals to make changes to data that the larger organization is unaware of. In contrast, blockchain relies on approvals from the majority of users to make changes to existing data, reducing the possibility of backdoor transactions on data.

Like the internet, blockchain has the potential to disrupt multiple industries and make processes more democratic, secure, transparent, and efficient. Some of the merits of this technology from a fraud prevention perspective are discussed below.

01. Blockchain can be used to create a potentially tamper-proof, cryptographically-secure online ledger that can be used to verify transactions securely and directly, on a peer-to-peer and decentralized basis, without the need for a middleman like a bank or financial institution.
02. Due to the decentralized nature of its networks, blockchain does not have a central point of failure and is expected to be better able to withstand malicious attacks.
03. Two parties can make an exchange without the oversight or intermediation of a third party, strongly reducing or even eliminating counterparty risk. Users can trust that transactions will be executed exactly as the protocol commands, removing the need for a trusted third party.

Sample benefits of blockchain adoption in select industries:

Healthcare – Regulate availability and privacy of health records

Defence – Critical defence information distributed across different locations can be secured more effectively

Government – Enables sharing of information amongst various departments that need the same data for different purposes

Law – Smart contracts (contracts enforced using blockchain) eliminate the middleman, such as a legal firm, as the payment will happen based on certain milestones being met. By its very nature, the smart contract is easily enforceable electronically, creating a powerful escrow by taking it out of the control of a single party

Insurance – A community of people, including payers, providers, claimants, and insurance companies, could be part of the overall blockchain, reducing fraud in insurance payments

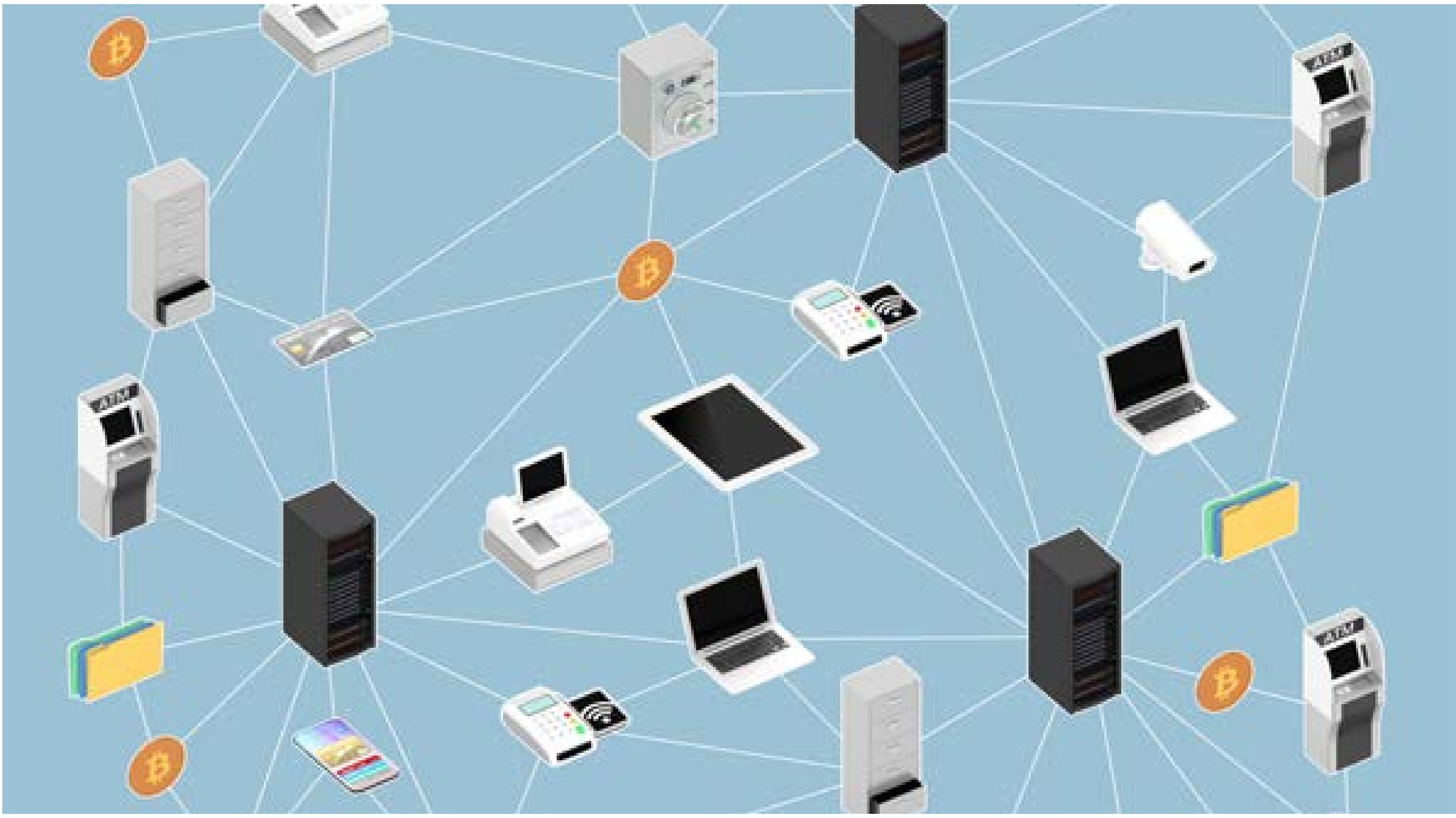
Source: http://www.oracle.com/us/corporate/profit/big-ideas/041316-siyer-2982371.html

However, the biggest challenge to blockchain adoption remains the absence of a centralized authority or regulatory system. Unlike the prevailing financial systems, blockchain does not grant full access rights over the network to any one user, administration or governing body and is hence difficult to regulate. This also means that users may have less avenues to seek redressal to fraud, malpractice or noncompliance on these networks. The possibility of a '51% attack', wherein a majority of Blockchain users could collude to wrest control of the blockchain, is a point of concern, although no such incidents have been reported so far. Also, security firms have argued that it is possible for individuals or groups to insert malware into blockchain transactions[17].

Lastly, questions remain over the integration of Blockchain with other technologies used by an organization, its customers and business partners. For Blockchain to work at an organizational level there is a need for re-designing business and application workflows, as well as adoption by all users.

At the time of writing this report, eleven banks of the R3 consortium had already connected to the centralized Ethereum-based blockchain network[18]. The Estonian government has been an early adopter of blockchain-based technology (keyless signature infrastructure) to authenticate data in their databases since 2013.

With such wide-ranging possibilities, blockchain has the potential to enhance outcomes with improved confidentiality and integrity of data. With its promise of providing secure and transparent transactions, blockchain seems poised to be one of the digital world's key pillars for fraud risk management.



[17] Source: http://www.rmmagazine.com/2016/03/01/the-risks-and-rewards-of-blockchain-technology/
[18] Source: http://www.nasdaq.com/article/r3-tests-its-blockchain-network-with-11-leading-banks-cm587878

Connected devices may not disconnect fraud - The Internet of Things (IoT) and its impact on fraud

What if your refrigerator has the ability to set temperatures depending on the perishables stored? Wouldn't it be convenient and save money on electricity bills? You can spend your time in other meaningful pursuits. But what if your refrigerator malfunctioned and short circuited itself, based on erroneous data that was provided to it clouding its judgement?

This is the power and the pitfall of the Internet of Things (IoT)–connected devices with inbuilt sensors that allow data exchange with other machines, enabling them to take decisions with minimal human intervention. Connected devices are programmed to collect huge amounts of real time data, process it and act as per set algorithms. What they aren't currently programmed for is to ascertain if the data provided is genuine or not.

An example of this was discovered in the banking industry. Several banks began using IoT-enabled ATMs to decentralize their ATM operations. Then, fraudsters discovered these IoT-based systems as a point of entry through which account balances could be accessed and manipulated. Through this control, fraudsters began to perpetrate any number of transactions. A common method involved withdrawing money from ATMs without having the balance of an account reduced, because the account was programmed to show unchanged balance[19]. This shows that computer network (on which these IoT devices primarily function) vulnerabilities and data privacy breaches are enough for devices to malfunction.

In many cases, physical dangers could also be a concern as machines increasingly make autonomous decisions at lightning speeds. For example, if network control points are not properly protected from a malicious attack, machines controlling airplanes, high-speed trains, cars or pacemakers could be compromised and cause physical harm[20].

We believe, the presence of these known vulnerabilities in the IoT ecosystem provides organizations with an opportunity to set the right internal controls in place so that they can leverage the benefits that connected devices offer, while mitigating risks. Some of these measures include:

- **Reviewing security and implementing data Governance** – When organizations connect devices to the cloud or to data centers to enable decision making, it poses the risk of confidential data being accessible to the outside world as well as the introduction of malware into the cloud. In light of this, reviewing and strengthening the current IT security infrastructure should be a priority. For instance, several companies tend to send their sensor data directly to the cloud or data center. This may create delays and drive up costs, in addition to opening up security risks. In such a scenario, organizations may have to re-look at the gateways they use.

  An untested area is whether IoT devices can 'spy'. For example a smart TV with an inbuilt camera being manipulated or whether a home security system can expose the patterns for the residents leaving or returning home. Some of these may extend into the work space as well.

- **Lack of data protocol standards**
  An IoT business model typically has three distinct facets: launch, manage, and monetize21. Across these stages, it is important to ensure consistent data standards across your organization (including aspects that may not directly deploy or rely on IoT technology). Some suggestions include:
  - Setting rate plans while integrating your IoT business with your existing infrastructure. Monitoring your connected devices in real-time, tracking data, usage, connectivity, etc.
  - Running diagnostics to identify and troubleshoot issues on any devices, anywhere, at any time.
  - Monetizing by setting rates for each type and level of service you offer and define how those plans will be managed over time, and then automate it.

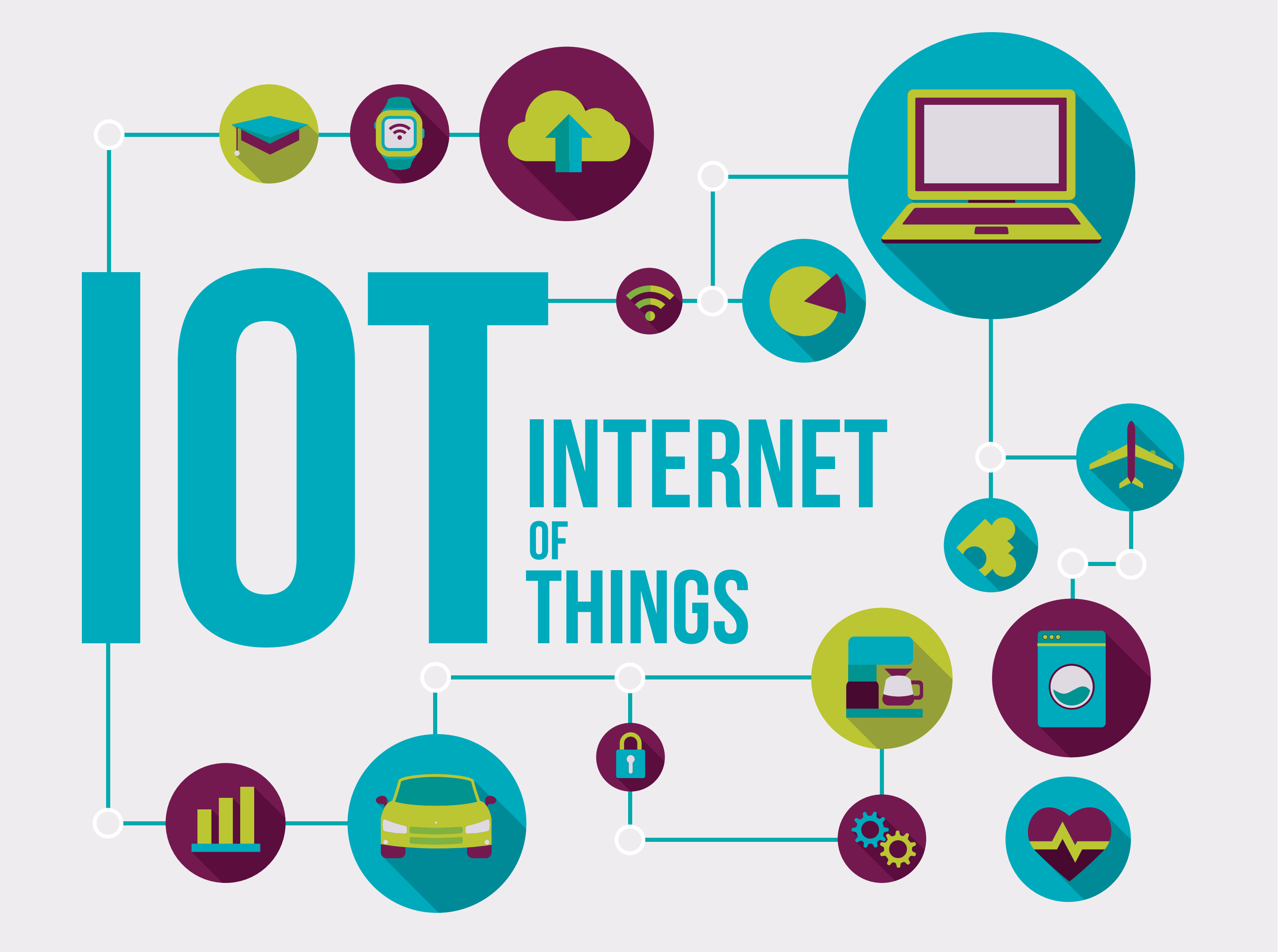
- **Identifying the right business and technology partners –** With many companies claiming to offer cutting edge IoT technology, organizations may feel overwhelmed and lost

[19] Source: http://synergy.syniverse.com/2016/09/understanding-emerging-fraud-internet-things/
[20] Source: http://www.rmmagazine.com/2014/02/01/preparing-for-the-internet-of-things-smart-devices-present-new-security-challenges
[21] Source: A whitepaper by Jasper Technologies titled Best Practices for Implementing Global IoT Initiatives, 2014/

while selecting a partner for IoT implementation. Considering some of the following aspects can help reduce fraud risks:

- Ascertain the business stability of the partner organization by understanding the background, financials and other clients serviced.
- Examine which IoT technology standard the provider has adopted and if the organization is using proprietary technology.
- Understand data hosting options on cloud such as public, private or hybrid cloud and choose the option that can best secure your data. Additionally, ascertain the ease of data storage, extraction, and availability of reporting tools.

The projected exponential growth of IoT[22] is likely to push organizations to adopt connected devices. Unless proactive steps are taken to address some of the known fraud concerns, large scale adoption of IoT in corporate India may see a rise in fraud.



[22] The IoT ecosystem is expected to be USD 15 Billion large by 2020, a three fold increase compared to 2016, according to a Deloitte Nasscom Report titled IoT – a Revolution in the making. Source - http://www.thehindubusinessline.com/info-tech/internet-of-things-market-to-touch-15-b-in-india-by-2020/article9189165.ece

Cashless transactions – are eWallets convenient or caution-worthy?

The recent announcement on demonetisation saw a flurry of people queuing up outside bank branches and ATMs, to either deposit their old currency notes or withdraw any denominations they could. What it also inadvertently led to was a rise in individuals and businesses adopting digital technology for transactions. A case in point was e-wallet providers reporting an overwhelming increase (in the region of 200% to 500%) in overall traffic, recharges, application downloads as well as a surge in average e-wallet balance, in just one day post the announcement by the government[23].

While electronic wallets are gaining popularity and usage, it is important to understand that there are inherent fraud risks and challenges (owing to the varied transaction models that exist as well as the technology used) that a user/ financial institution may be affected by. These could be[24]:

- **Phishing fraud -** Fraudsters may use phone calls, SMS messages, or email to trick users into divulging their PINs or other personal information that may result in embezzlement of virtual money from the wallet. The customer may also transfer virtual money himself under false promises or schemes.
- **Intrusion/Cyber Attack -** Fraudsters may hack into the mobile money platform and manipulate wallets to their gain. This could be caused by either inadequate IT securities or having an understanding of the architecture and gaps in infrastructure of the wallet platform.
- **Unauthorized SIM swap -** A fraudster may attempt to take over someone else's mobile wallet account by pretending to be that person using false identity documents. Once they assume the other person's identity, they are able to swap SIM cards and obtain full access to funds.
- **Fake KYC -** Customers can furnish fake KYC documents to gain access to premium wallets that allows higher transaction value (transfer and cash out). This may help facilitate money laundering.
- **Commission frauds by agents (Introduce fake accounts/perform split transactions) -** Mobile money agents may try to earn more for themselves by breaking up legitimate customer transactions into smaller ones. By doing so, agents can earn more commissions as a result of higher transaction volumes. Agents may also introduce fake accounts to gain higher registration commissions.
- **Benefits through misconduct -** Regular customers can discover product or application flaws that can provide benefits to them in a specific scenario and can repeatedly simulate the same scenarios to exploit these limitations. For example transaction failures for specific scenarios results in wallet/ account getting credited without corresponding debit from the other side; referral bonus on already registered customers; avail bonus on refill of wallet, without actually recharging/ refilling; avail discount on same merchant transaction.

As is evident from the above, most of the key root causes are a result of internal control failures around governance, IT and continuous monitoring, making regular fraud review and monitoring a mandate. With the mobile payments industry being largely at a nascent stage in India, the ultimate surge in mobile platform adoption rates may be accompanied by a spate of fraud risks. Organizations therefore, while focusing on building a user base, also need to look into adopting fraud control measures. In our experience, each stakeholder in the mobile wallet value chain tends to look at risks in isolation, limiting the preventive measures to their immediate area of operations.

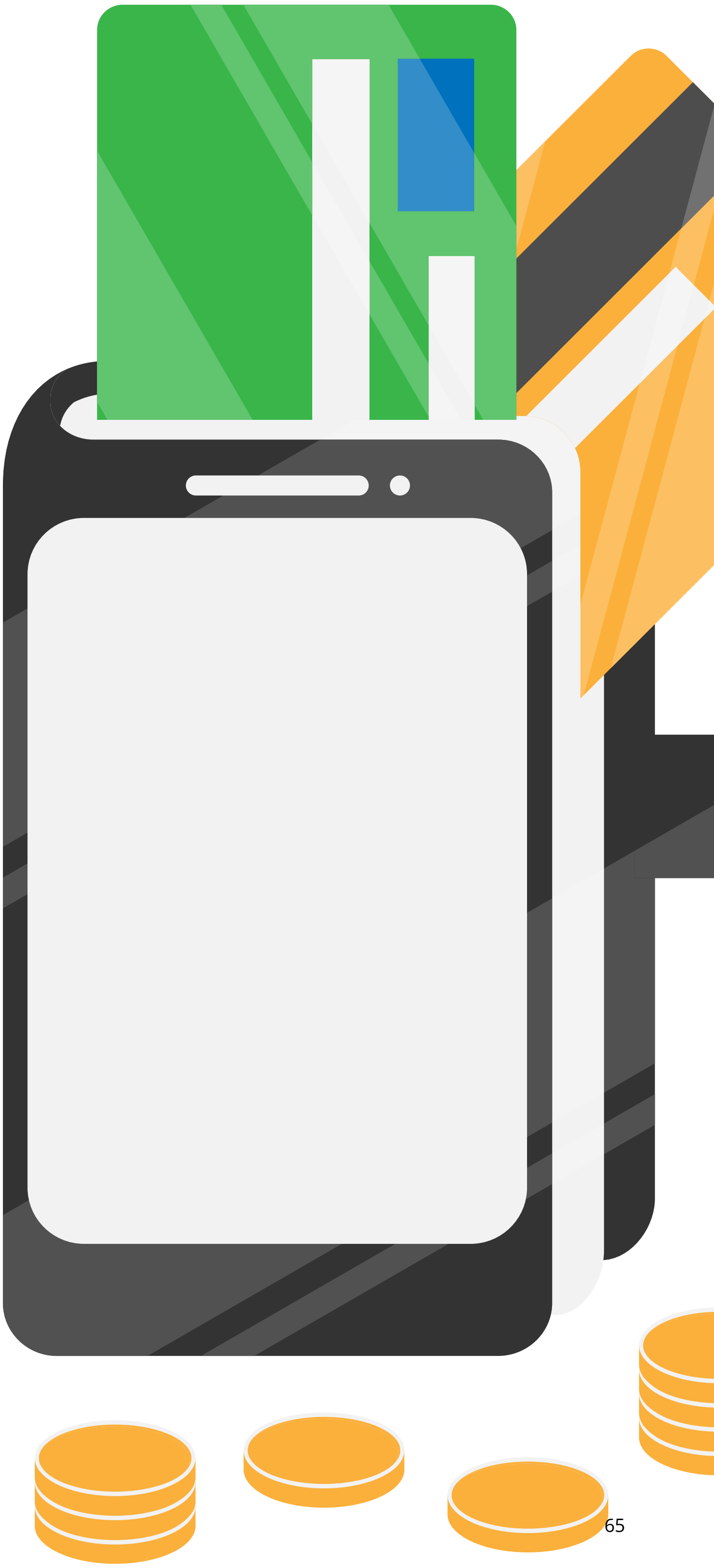
A more robust fraud mitigation approach would involve deriving synergies from respective stakeholders (banks, telecom companies, etc.) and integrating them to build a robust, comprehensive fraud risk management framework. In our view, the success of such an integrated approach to fraud risk

[23] Source: http://techcircle.vccircle.com/2016/11/09/digital-wallet-firms-see-unprecedented-growth-after-ban-on-high-value-notes/
[24] Source: Deloitte India point of view document titled 'Mitigating emerging fraud risks in the mobile money industry', 2015

management in the mobile wallet industry rests on three pillars:

- **Strong foundation -** Coordinated SDLC (System Development Life Cycle) Governance - Organizations need to take cognizance of all possible fraud scenarios while developing the products or application. User Acceptance Testing (UAT) needs be comprehensive to cover all exceptions and fraud scenarios and tested not only by business users from all entities, but also independent control functions. The roles and responsibilities between organizations and departments needs to be clearly defined, including accountability in case of any fraud incidence.
- **Leveraging data analytics to build a fraud indicator dashboard for robust monitoring -** Building upon the learnings from Risk Analytics in the Banking sector and Fraud Management Systems in the Telecom sector, mobile wallet companies can develop a Fraud Indicator Dashboard to help in early detection of red flags. Such a dashboard can help provide real time fraud alarms on customer transactions and internal violations, enable customer profiling, provide analysis to strengthen product gaps, etc.
- **Effective consequence management -** Organizations need to set the right tone at the top and exercise strong disciplinary action against identified suspects. It is also important to have a sound process to manage customer grievances due to fraud and transfer accountability to the party responsible for this.

(A version of this write-up was contributed to the Forbes Online magazine at the time of writing this survey. It was published here - http://www.forbesindia.com/blog/economy-policy/switching-to-the-online-route-is-all-well/)



Robotics – Will the final frontier be fraud free?

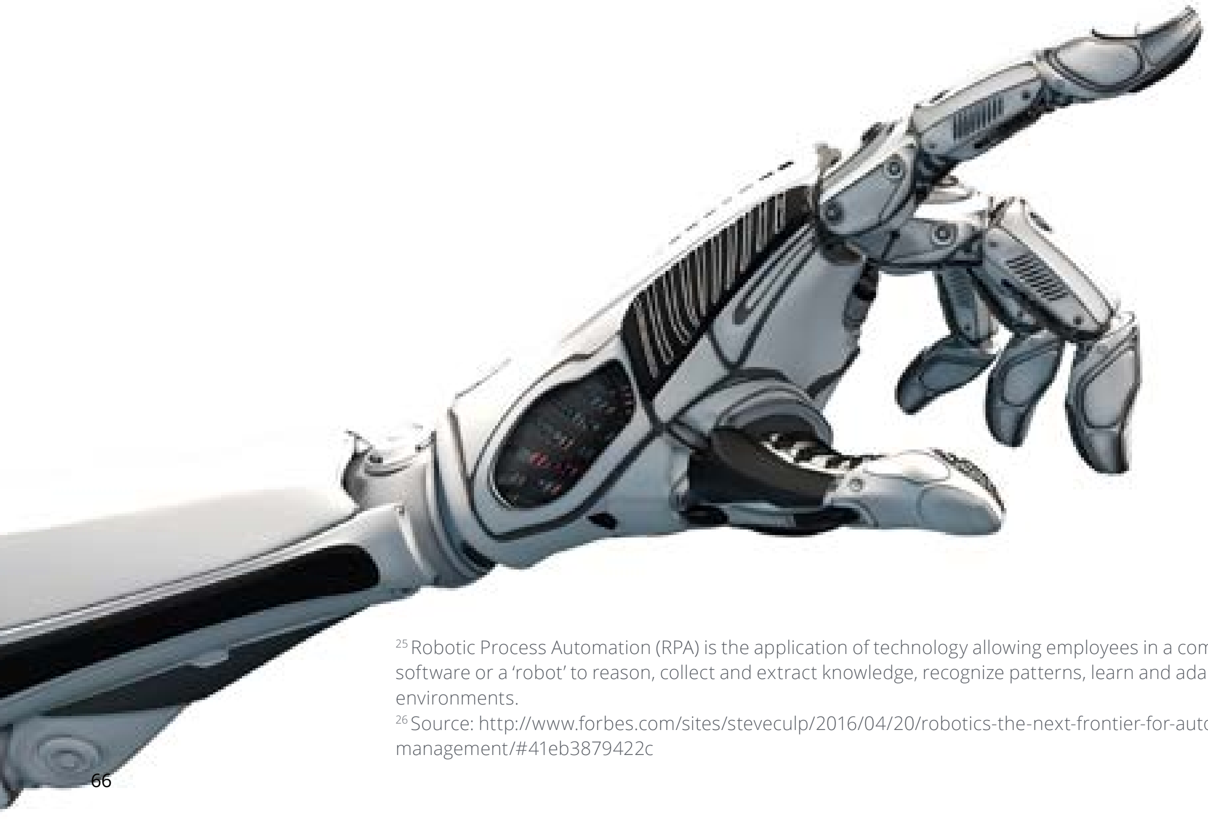
Robotic process automation (RPA)[25] or intelligent automation (the combination of artificial intelligence and automation) is starting to change the way business is done. RPA leverages recent software abilities made possible by breakthroughs in computing power, including natural language processing, machine vision, and speech recognition.

As a result, such systems can detect and produce vast amounts of information and automate entire processes or workflows. Until recently, robotics had its applications in human intensive sectors such as manufacturing, where it automated processes such as assembly line, warehousing and cargo bay operations, resulting in improved performance and safety.

In recent times, though, robotics is seeing applications in other sectors too. Financial services, for instance, is seeing the adoption of robotics to streamline operations and ensure appropriate levels of control. In the finance and accounting areas, robotics can be used for fixed-asset accounting, to record journal entries, conduct general ledger account reconciliation, perform intercompany transactions, and maintain accounting master data[26].

While there are obvious benefits to introducing robotics and artificial intelligence into business, there are also potential fraud risks that organizations need to be aware of. There has been a rise in the number of frauds related to high technology corresponding to the rise in the number of individuals, networks, corporate intranets, Internet, National Information Infrastructure (NIIs), and global information infrastructure (GII) access points. More networks mean that more people have access to more information. Some of those who have this access, both legal and illegal, can compromise these systems. High-technology frauds are therefore expected to continue increasing in the future–both in the number of incidents as well the quantum of impact. As robotics technology evolves, we expect these frauds to become more sophisticated. Some of the following controls may help mitigate fraud arising from robotics adoption:

- Putting access controls in place so that only authorized individuals can access information. When necessary, these controls may need to be backed by multi-factor authentication.
- Data Encryption on devices can transform customer information into unreadable text, so when transmitted, it cannot be read by cyber-criminals.
- Monitoring Procedures can be put in place to look for evidence that cyber-criminals have accessed, or attempted to access, customer information.
- Environmental Hazard Protections-If required, such protections guard against technology failures or actual physical damage that could leave customer information vulnerable.
- Supporting devices or equipment (e.g. high-technology devices) available/ installed to meet new fraud threats.



[25] Robotic Process Automation (RPA) is the application of technology allowing employees in a company to configure computer software or a 'robot' to reason, collect and extract knowledge, recognize patterns, learn and adapt to new situations or environments.

[26] Source: http://www.forbes.com/sites/steveculp/2016/04/20/robotics-the-next-frontier-for-automation-in-finance-and-risk-management/#41eb3879422c

Online market places – Can B2B businesses match the B2C success on these platforms?

The Indian government is likely to adopt an online market place model for all government purchases–from paper clips to power plant turbines[27]. While this initiative is expected to curb corruption, improve transparency and competitiveness, and incur savings of at least 10%, the bigger question is–how safe will this market place be? After all, popular e-commerce market places deploying online security measures have fallen prey to fraud in the past.

Online payments and procurement of materials were identified as areas vulnerable to fraud risks in e-commerce transactions, according to survey respondents of our 2014 fraud survey. 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 transaction[28].

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 purchased[29]. 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, other fraud risks, such as leakage and loss of confidential data, fraudulent transactions, and inadequate security at payment gateways, can deter 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.

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

01. 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. Several government websites have in the past been replicated on these models, leading to loss of citizen data.

02. Credit card chargeback: Chargeback refers to a scenario when a customer disputes the amount charged on his/her credit card and refuses to honour 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. Currently, disputes with the government tend to be long drawn out before they can be resolved. How an online market place will respond to this challenge remains to be seen.

03. 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. Currently, several states in India have implemented e-procurement and continue to face several challenges including misleading information shared by companies bidding for work and the inability to assess the quality of purchase, among other challenges[30].

[27] Source: http://www.livemint.com/Industry/wrHeksCE7XtA5wc1g6GGIM/Modi-bids-to-cut-corruption-in-India-with-Amazonlike-online.html

[28] Source: EMC- RSA Research - http: //www.emc.com/collateral/fraud- report/rsaonline-fraud -report-0714.pdf

[29] 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=Ecommerce%
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.Josep
h,+Page+50&source=gbs_toc_r&cad=4#v=onepage&q=Ecommerce%2C%20an%20Indian%20perspective%2C%20second%20edition%2C%20
by%20P.T.Joseph%2C%20Page%2050&f=false

[30] Source: http://www.thehindu.com/news/cities/bangalore/states-eprocurement-system-not-reliable-cag/article8403664.ece

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 organizations can adopt to have a safer e-commerce experience while transacting with the government include the following:

01. **Establish anti-fraud policies and procedures:** The government can have a comprehensive and clear policy on aspects such as bidding, awarding of contracts, online payments, and returns/ dispute management. Further, a manual that identifies potential fraud risks and noncompliance may help weed out suspicious bidders. Buyer organizations can have a similar policy that details how to identify genuine government 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.

02. **Forming a dedicated team to monitore-commerce market place 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 identify emerging frauds is an effective strategy, given the evolving nature of e-commerce business in India. The government can deploy third parties to undertake such periodic checks. Organizations, on their part, can report any suspicious incidents to the government.

03. **Due diligence:** Given the large third party ecosystem that supports e-commerce in India, the government needs 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 bidders/contractors. Bidding organizations can also conduct due diligence on requests for proposal to ensure that they are transacting with government departments and not fraudsters.

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. Until the time India sees similar legislation, e-commerce transactions – whether with the government or any third parties–are likely to be risky. Organizations therefore, need to take measures to ensure that they are adequately prepared to tackle these fraud risks.

CREDIT CARD
1234 5678 9012 3456
VALID THRU
Firstname Lastname

Foreign perspectives on dealing with fraud in India

Poor anti-fraud controls at Indian partner organizations a concern - Perspectives from Japan

(This section has been authored by Deloitte Tohmatsu Financial Advisory LLC in Japan. It is independent of the findings of the India Fraud Survey, edition II.)

According to research by Japanese embassies in India and the Japan External Trade Organization (JETRO), the number of Japanese companies expanding their businesses in the Indian market has been consistently increasing over the last few years[31]. While the Indian market offers unique opportunities for Japanese companies in business, rising instances of corporate fraud as well as the management of such fraud by Indian organizations, is a concern for Japanese companies. Around 38% of respondents to the fraud survey conducted by Deloitte in Japan (in October 2016), indicated that fraud at overseas subsidiaries was a key concern for the future.

This is a marked difference from the past, where Japanese companies were concerned primarily about physical business risks, such as the difficulties in establishing a supply chain due to infrastructure limitations in India. However, recent incidents of fraud in India involving Japanese company subsidiaries have resulted not just in monetary losses but also loss of reputation, owing to the publicized nature of some of these frauds. While relatively simple frauds, such as theft by employees, continues to plague Japanese companies operating through Indian subsidiaries, what is worrying is the involvement of local business partners in fraud schemes in the past. We have observed that many of the Indian local business partners tend to be family owned/ operated. Often, these partners may be directly involved in frauds such as misappropriation of assets and financial statement frauds so as to divert money to multiple family/related businesses. Further, the average loss due to such frauds tends to be larger than other frauds that we see in Japan.

[31] http://www.in.emb-japan.go.jp/Japanese/2015j_co_list.pdf

The state of corporate fraud in Japan

26%
of respondents acknowledged that they experienced some type of frauds in the past three years

Top fraud concerns: Asset misappropriation	**57%**
Financial statement fraud	**26%**
Corruption	**10%**

Fraud loss due to asset misappropriation tended to be less than JPY 10 million, whereas that due to financial statement fraud and corruption was more than JPY 100 million for many cases

Anti-fraud measures taken by companies include establishing whistle-blower hotlines, conducting employee training, and performing internal audit procedures

Fraud concerns for the future include cyber-attack/ information leakage (52%) and frauds at overseas subsidiaries (38%)

Information source: Deloitte Japan Fraud Survey 2016

[31] http://www.in.emb-japan.go.jp/Japanese/2015j_co_list.pdf

This has created a perception that doing business in India is risky[32] and that anti-fraud controls (such as those deployed by the parent companies in Japan) may not be effective against fraud, especially if managed from Japan. This is one of the reasons Japanese companies prefer to send executives from Japan to work in India and directly monitor business activities through physical presence. At the same time, Japanese companies also recognize the need to strength their internal controls, including anti-fraud controls and programs, at its Indian subsidiaries. However, due to limitations on resources and budgets, Japanese companies are often unable to secure themselves adequately in India.

Many Japanese companies are aware that Indian regulators are moving towards strengthening compliance issues (for example, mandating the need for a vigil mechanism such as whistleblowing hotlines public companies, as part of the Companies Act, 2013). However, many Japanese companies' business partners tend to be family owned/ operated (i.e., not a public company) and the perception is that it may be difficult for Japanese companies to benefit from such regulations. Furthermore, there is also a perception that the Indian judicial system is complicated and takes a long time to resolve issues, particularly those around corporate fraud. These concerns are making it challenging for Japanese companies to deal with fraud in their Indian subsidiaries. We look forward to better enforcement of legislation and adoption of anti-fraud controls at partner organizations.

[32] Compared to other developing markets

Spotlight on supply chain crises – Perspectives from Australia

(This section has been authored by Deloitte Risk Advisory Pty Ltd Australia. It is independent of the findings of the India Fraud Survey, edition II.)

"Our people are our greatest asset" is an often used platitude in business these days. But what about when these greatest assets become a business's greatest risk and trigger a major crisis?

Supply chain crises are well-known and documented. Some recent crises have included the Bangladesh factory collapse, in which prominent elite branded apparel was on display within the dirt and rubble. Then there was the horse meat scandal that rocked the leading supermarket chains in the United Kingdom. More recently in Australia, there was the hepatitis A scare that was blamed on imported Chinese berries – which has yet to be confirmed.

These types of crises, involving supply chains, have common elements that relate to the product being of an inferior than purported standard and the potentially dubious work practices of the foreign upstream manufacturer. These elements have a material impact when the brand and reputation of a business are associated with the product, but are often dismissed as being an "over there" problem (while accompanied with an arm-waving gesture in the vague direction of the country to blame).

One emerging crisis trigger that cannot be as easily dismissed is the issue of the workforce triggered crisis. Like key business value drivers such as data, communications, facilities, access, and good leadership, a reliable workforce is a critical element to most successful businesses. The workforce is a key ingredient in operations of many horticultural, retail, manufacturing, mining and service businesses. If the workforce becomes unavailable, the business will quickly fall off the edge of a financial cliff.

The outsourcing of the provision of the workforce is done through a range of third-party providers but can also be done through the franchise model of business. In the latter case, the workforce is hired by the franchise owner, which is usually at arm's length and unseen by the franchisor (or head office). Regardless of the model, the risk and any subsequent crisis, remains firmly attached to the brand and reputation of the overall business. Also, the workforce is usually the public face of the business, wearing branded uniforms, engaging with customers, and holding the business's reputation in their hands when asked by friends and family the perennial question, "how's work going?" But, with a global economy and a far more mobile workforce, there has been an increase in the need to outsource the supply of this workforce to third-party employment agencies. Here lies the foundation of a crisis.

With over 100,000 non-resident workers in Australia holding 457 temporary work or student work visas, it is becoming even more important that businesses are alert to the potential risks, should these workers or their employment agencies deliberately (or inadvertently) breach the conditions of the visas. Such a breach can lead to deportation of the worker and fines from the immigration authorities for the employer and the agency, but it is the brand damage done in the process that is the real cost.

A knock-on impact beyond the brand and reputation damage is the supply chain impact. What has been seen in recent workforce crisis situations is that if these foreign workers become concerned that the immigration agencies will swoop at any moment, they will not attend work, causing a significant workforce shortage and a rapidly approaching abyss for the business. Organizations therefore need to safeguard themselves from these potential crisis situations through investments in better planning and data analytics.

Acknowledgements

We would like to thank the following people whose efforts shaped this survey report: Ajay M.P., Ajit Nathaniel, Akriti Bhatnagar, Anindita Singh, Anurag Datta, Archana Venkat, Asha Lexmi Moorthy, Badri Narayanan GR, Bhavya Arora, Chaitali Dhiman, Darpan More, Devika Mistry, Gaurav Lall, Himanshu Arora, Jitendra Dadlani, Nandini Mathur, Navaz Dubash, Nithya Manohar, Rini Roy, Ritika Shah, and Shweta Todankar.

We would also like to thank the Information Technology and Brand and Communications teams at Deloitte India and the Quality and Risk team at Financial Advisory Services, Deloitte India, for supporting us with this document.

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 and companies working in the area of fraud risk management, as well as working professionals, in October and November 2016. The response rate to questions varies and not all respondents have answered all questions in their respective surveys.

The three surveys-focused on large (domestic and multinational) companies, small and medium enterprises and working professionals- saw a total of 309 responses.

Each statistic used in this report is derived from the number of responses to that question and must not be considered consistent across the report. For multiple choice questions and priority based questions, the weighted average of responses for that question has been used to derive the statistics.

Key contacts

Rohit Mahajan
APAC Leader
Partner and Head, Forensic
Financial Advisory, Deloitte India
T: +91 22 6185 5180
E: rmahajan@deloitte.com

Amit Bansal
Partner
Forensic - Financial Advisory
Deloitte India
T: +91 22 6185 6764
E: amitbansal@deloitte.com

Jayant Saran
Partner
Forensic - Financial Advisory
Deloitte India
T: +91 124 679 3607
E: jsaran@deloitte.com

K. V. Karthik
Partner
Forensic - Financial Advisory
Deloitte India
T: +91 22 6185 5212
E: kvkarthik@deloitte.com

Nikhil Bedi
Partner
Forensic - Financial Advisory
Deloitte India
T: +91 22 6185 5130
E: nikhilbedi@deloitte.com

Rajat Vig
Partner
Forensic – Financial Advisory
Deloitte India
T: +91 124 679 2905
E: rajatvig@deloitte.com

Sumit Makhija
Partner
Forensic - Financial Advisory
Deloitte India
T: +91 124 679 2016
E: sumitmakhija@deloitte.com

Directors within Deloitte Forensic's practice in India

- Ajay Singh (ajaysingh@deloitte.com)
- Arjun Rajagopalan (rarjun@deloitte.com)
- Nishkam Ojha (nojha@deloitte.com)
- Rahul Kalia (rkalia@deloitte.com)
- Rajesh Chawla (rajchawla@deloitte.com)
- Rohit Goel (rogoel@deloitte.com)
- Rohit Madan (madanr@deloitte.com)
- Sebastian Edassery (edasserys@deloitte.com)
- Somyajit Sethi (ssomyajit@deloitte.com)
- Sushmit Bhattacharya (bsushmit@deloitte.com)
- Veena Sharma (vesharma@deloitte.com)
- Wilfred Bradford (wbradford@deloitte.com)

Deloitte.

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 survey is carried out by Deloitte Touche Tohmatsu India LLP (DTTILLP) and data or information provided by you will be used in connection with this survey, other studies or analyses performed by DTTILLP. This survey and the survey results are the proprietary property of DTTILLP and will be disclosed only if required by law or in connection with this survey or such studies, analyses or services, however the data or information provided would not contain any information that identifies you or associates with you the responses you have provided.

This survey and the general information contained 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 you or your 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 or entity by reason of access to, use of or reliance on, this survey or the survey results. By using this material or any information contained in it, the user accepts this entire notice and terms of use.

DTTILLP do not express an opinion or any other form of assurance. Further, the survey results/information in this document are not intended, nor should they be interpreted to be legal advice or opinion.

DTTILLP will not under any circumstances be liable for any direct, indirect, incidental, consequential, punitive or other damages, whether in an action of contract, statute, tort (including without limitation, negligence) or otherwise, relating to the survey results/information contained herein and/or the use of the survey results/information contained herein.

This document may contain information from secondary sources of published information and may incorporate the inputs gathered through meetings with various industry experts and other industry sources, which for reasons of confidentiality, cannot be quoted in this document. DTTILLP does not undertake responsibility in any way whatsoever to any person or entity in respect of errors in this document, arising from incorrect information provided by the industry experts/sources and/or other sources.

While information obtained from the public domain has not been verified for authenticity, DTTILLP have endeavored to obtain information from sources generally considered to be reliable. DTTILLP assume no responsibility for such information.

DTTILLP's survey results/information in the document is based on the prevailing regulatory environment and any change may impact the outcome of DTTILLP's survey. Further, such survey results/information indicate only that DTTILLP have undertaken certain analytical activities on the underlying data to arrive at the survey results/information presented in the document; DTTILLP do not accept responsibility or liability for the underlying survey results/information."