

PwC's Global Economic Crime Survey 2016

An India perspective



31%

of the respondents in India have experienced economic crime in the last two years

56%

of the Indian respondents perceived an increased risk of cybercrime over the past two years

61%

of economic crimes in India are committed by employees within an organisation



Contents

8



*The India story:
Charting the
landscape
of economic
crime*

*Greater
opportunities
for economic
crime in India*

14



28



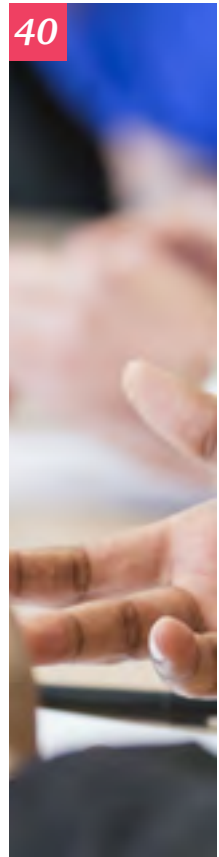
*New weapons
of mass
destruction*

*Countering
fraud: Business
ethics and
compliance
programmes*

36



40



*Last word:
From crisis to
opportunity*

***Stay alert.
Stay ahead.***

Counter economic crime. Ensure business growth.



About the survey

PwC's Global Economic Crime Survey is one of the most comprehensive studies of economic crime in the business world. This year, we received more than 6,000 responses from around the world.

In India, our survey respondents are from various industries and sectors. A diverse mix of views from senior executives across a range of functional specialisations from listed, public and private sector organisations makes this survey representative of corporate India's perception of economic crime.

With economic crime being seen as a serious threat globally, it is time for organisations and business leaders to arm themselves for the fight against fraud. The key message is to be forewarned and forearmed to counter economic crime in the current business environment.



Dinesh Anand
Partner and Leader
Forensic Services, India

Foreword

I am pleased to present the first-ever **India edition** of PwC's Global Economic Crime Survey. Comprising diverse points of view across 17 industry sectors, this report provides a complete and holistic picture of economic crime in India.

The 2016 survey shows that economic crime remains a serious concern. The survey not only puts into focus the impact of evolving regulatory requirements and technology on economic crime, but also re-emphasises the increasing difficulties of predicting and detecting economic crime.

We hope that this report will help business leaders navigate the increasing complexity around economic crime. As India continues to evolve into a major economic power, we hope that this report will encourage debate and equip businesses with the skills to deal with challenges related to economic crime.

I would like to express my sincere gratitude to all the participants of the survey. I hope you find the report useful and insightful.

Best regards,

A handwritten signature in black ink, appearing to read 'Dinesh Anand', written over a horizontal line.



The India story

Charting the landscape of economic crime

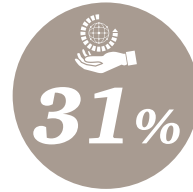
Continuous growth

With India having topped the World Bank's growth outlook for 2015–16 for the first time and achieved economic growth of 7.3% in 2014–15, there is an upsurge of optimism in business corridors. The Indian government has introduced a series of policy reforms and regulatory interventions that have been welcomed by corporate India. The country continues to be one of the most popular business destinations, attracting foreign investments from across the globe.

Rise in economic crime

Although the general business sentiment remains positive, the threat of fraud, bribery and corruption looms large. Our survey tells us that **more than one in every four organisations in India are impacted by economic crime**—a finding that reflects the pervasiveness of the problem in India.

With the spike in cybercrime, cyber readiness is fast emerging as one of the key areas of concern for businesses across India. Cyber security disclosure norms are conspicuous by their absence, and there is an urgent need for robust mechanisms that can curb the increasing instances of cyber security breaches. Fittingly, **44% of the respondents in India felt that local law enforcement agencies do not have the required skills and resources to investigate cybercrime, hacking incidents and malware-related fraud.**



of the respondents in India have experienced economic crime in the last two years



of the Indian respondents perceived an increased risk of cybercrime over the past two years



of economic crimes in India are committed by employees within an organisation

A few positive developments

Recently, a few regulatory changes were introduced to improve transparency and promote ethical business practices. With the introduction of the Black Money (Undisclosed Foreign Income and Assets) Imposition of Tax Act, 2015, the Benami Transaction (Prohibition) Amendment Bill, 2015, and the Companies (Amendment) Act, 2015, measures are in place for the penalisation of prohibited and unethical business activities. These are steps in the right direction.

In this environment of rising economic crime and regulatory changes, it is interesting to see self-regulation emerge as one of the key trends. As businesses interact with the government and civil society in new ways, we find that they are voluntarily adopting rules related to ethics and compliance.

Our survey reveals that 88% of organisations in India have a formal business ethics and compliance programme, and 56% have seen an increase in their spend on compliance programmes and resources.



PwC India Speak

Dinesh Anand
Partner and Leader
Forensic Services
India



'We see an increasing aspiration among Indian businesses to move beyond statutory compliance into the domain of self-regulation. Many companies no longer want compliance to be just a “tick in the box” exercise. We see them invest more and more in comprehensive compliance and monitoring programmes, especially around ethics and fraud, as their first line of defence against economic crime.'



Key survey findings

1

The problem is real

- **31%** of the Indian respondents experienced economic crime in the last two years.
- **27%** of the participating organisations in India were asked to pay a bribe in the last two years.



2

Law enforcement needs to step up

- Almost **50%** of the respondents in India felt that local law enforcement agencies are not adequately resourced and trained to investigate and prosecute economic crimes.



3

Cybercrime is here to stay

- **56%** of the Indian respondents perceived an increased risk of cybercrime over the past two years, as compared to 53% globally.
- **16%** of the organisations experienced cybercrime in the past two years.
- Only **45%** of the organisations have fully trained cybercrime first responders.



4

Renewed focus on ethics and compliance

- **88%** of the responding organisations in India have a formal business ethics and compliance programme.
- **56%** of the responding organisations witnessed an increase in their spend on compliance programmes and resources.



5

Difference between perception and reality

- **94%** of the Indian respondents stated that their organisations had a clear code of conduct.
- However, **15%** indicated their leaders did not walk the talk, **24%** mentioned unclear communication and training, and **19%** feared retaliation for reporting a violation.



6

Who drives crime perpetration

- **61%** of the respondents in India believed that the main perpetrator in the most serious economic crimes detected were internal to the organisation.
- The survey presents the following profile of a fraudster: a highly educated/educated male between 31–40 years at a junior to middle level in the organisation.







PwC India Speak

Gagan Puri

Partner
Forensic Services
India

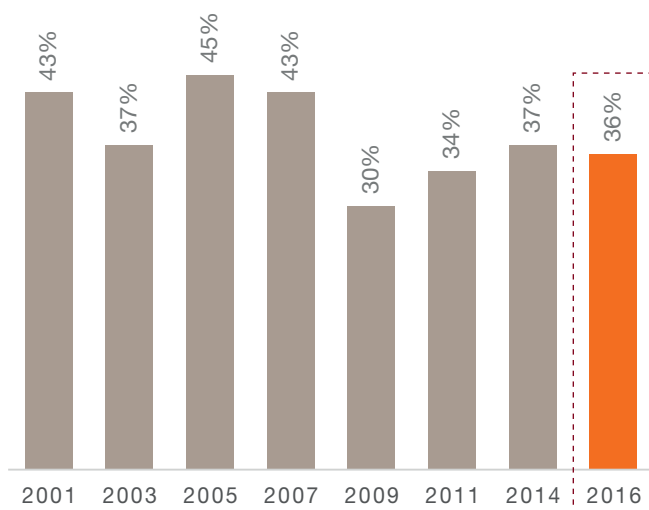


'Our experience in the last few years is broadly consistent with the results of the survey. However, one additional area where we see significant activity is economic crime perpetrated by senior management. When such a crime takes place, the amounts involved are huge, complex determination is required, and regulatory and other reporting obligations are triggered in India and, in many cases, in foreign jurisdictions. From a crisis management perspective, it takes significant efforts on the part of companies to effectively resolve and address these situations.'



Greater opportunities for economic crime in India

Global economic crime trends



While 65% of the respondents in India and 59% of the global respondents encountered less than 10 separate incidents of economic crime, it is pertinent to note that a quarter of the Indian respondents who experienced economic crime (compared to more than a fifth of the global respondents) encountered between 11 and 100 separate incidents of economic crime. A further 6% of the Indian and 9% of the global respondents encountered more than 100 separate economic crime incidents during the last 24 months.

PwC India Speak

**Arpita Pal
Agrawal**
Partner
Forensic Services
India



'The survey on the number of incidents of economic crime highlights a very important issue from an Indian perspective, which is multiple and repetitive instances of economic crime. Perpetrators are becoming increasingly innovative and bold when it comes to their modus operandi. However, organisations appear to be mostly in a reactive mode, plugging gaps selectively. The absence of directed company-wide efforts to contain economic crime is one of the main reasons for increased perpetration.'



of the respondents in India have experienced economic crime within the last 24 months

as compared to

of the organisations globally

Types of economic crime

Asset misappropriation was the most common type of economic crime in India over the last 24 months, followed by procurement fraud and bribery and corruption.

What type of economic crime has your organisation experienced in the last 24 months?

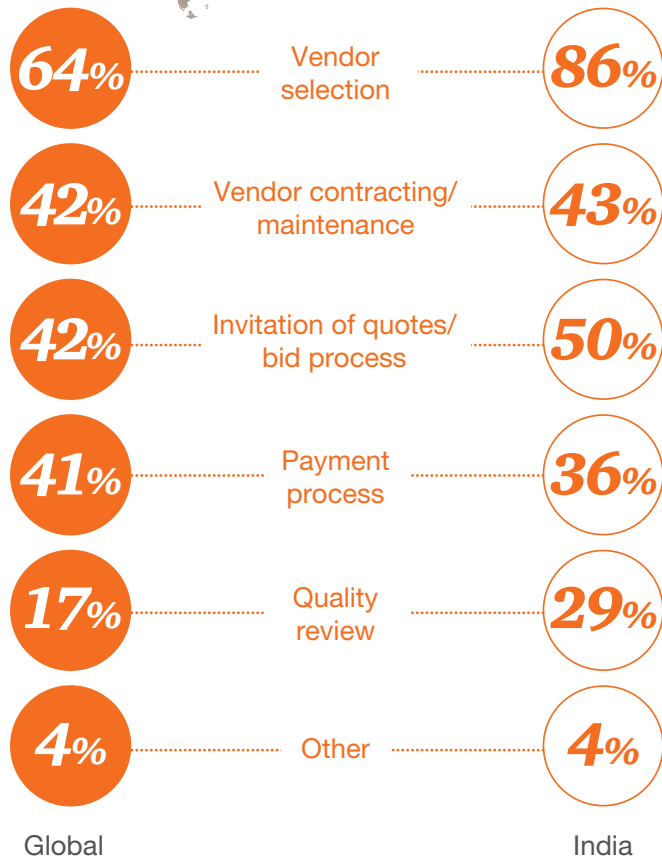




Trends in procurement and human resources frauds

The survey results pertaining to these types of fraud, in our opinion, indicate the areas where organisations need more stringent controls.

Procurement fraud





In the Indian context, these results suggest that vendor selection continues to be the most significant area in the respondents' organisations, followed by inviting quotes/bid process and vendor contracting/management.

PwC India Speak

Darshan Patel

Partner
Forensic Services
India



'It is no surprise that procurement fraud remains one of the significant areas of concern for corporate India. Our investigation on some of the biggest cases in this area has revealed increasing instances of personal profiteering with increasing spends by companies. However, perpetrators have become much smarter, thus making detection a huge challenge. In today's environment, one is less likely to find an obvious email or SMS trail related to unethical activity in people's inboxes but more likely to find larger kickbacks routed through a complex network of entities held in the "beneficial interests" of internal perpetrators.'



Human resources frauds

With regard to key types of fraud in the domain of human resources, 44% of the global respondents identified submission of false qualifications, and 27% addition of ghost/fictitious employees to the payroll. Further, respondents stated that falsification of entitlement/employee benefits (32% globally), false wage claims (e.g. commission; 40% globally) and other sub-processes (39% globally) are also common.

PwC India Speak

Puneet Garkhel
Partner
Forensic Services
India



'Machines do not commit crimes—the people manning those machines are responsible.

Today, corporate India recognises people as a threat from within. We launched our strategic threat advisory practice last year and have assisted organisations in mapping strategic threats from a variety of resources. Apart from the people-related risks mentioned in the survey, we see huge concerns around threats emanating from sources such as physical security, terrorism, social engineering and travel.'

Financial damage



The true cost of economic crime to the Indian economy is difficult to estimate, especially considering that actual financial loss is often only a small component of the fallout from a serious incident. Business disruptions, remedial measures, investigative and preventative interventions, regulatory fines, and legal fees, among other factors, have an impact on the bottom line, and these costs can be enormous, although they are largely inestimable.

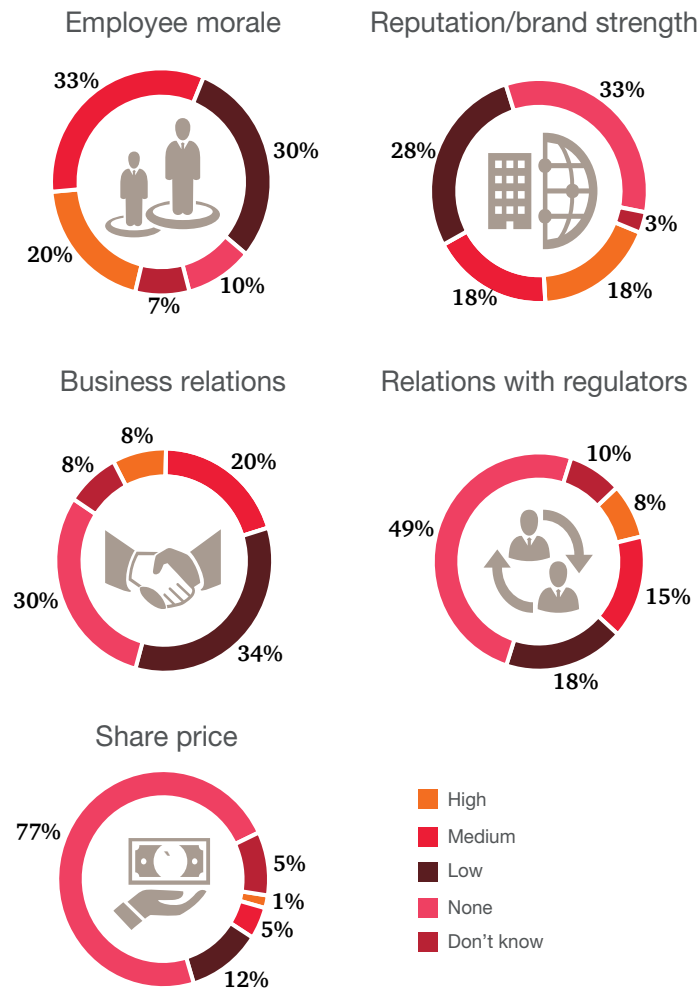




Collateral damage

Incidents of economic crime mainly impact employee morale, brand strength, business relations and share price of the organisation.

Within the last 24 months, what was the impact of economic crime experienced by your organisation on each of the following aspects of your business operations?





PwC India Speak

Rahul Sogani

Partner
Forensic Services
India

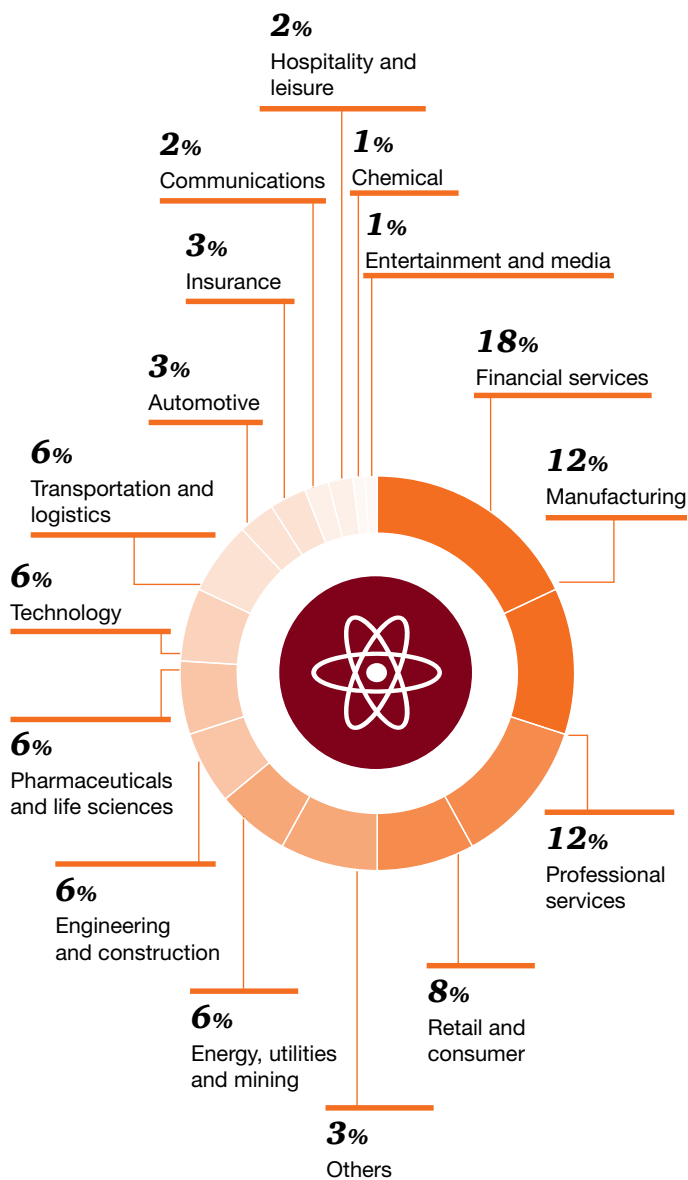


'In our opinion, one of the biggest costs of a fraud is damage to reputation. It is not easy to cope with the loss of a senior employee, a trusted business advisor or a major business relationship, or with loss of confidence from investors, regulators or stakeholders. In addition, there is the cost of remediating the problem, dealing with the crisis, and rebuilding confidence and trust, as well as the toll on internal and financial resources. So, one ends up spending a significant amount. An economic crime perpetrated in today's environment can rapidly evolve into a full-time assignment for senior management, with repercussions on day-to-day business.'



How is economic crime affecting the industry spectrum?

Within which industry does your organisation mainly operate?





Financial services has traditionally proved to be the industry that is most susceptible to economic crime—particularly since it is the only industry that serves the financial needs of all the other industries.

However, with the market evolving towards integrated business solutions, many traditionally non-financial services organisations are now coming into their own by providing for the financial requirements of their clientele in-house. Numerous non-financial services businesses in the automotive, retail and consumer, and communications sectors, to name just a few, are either in joint arrangements with financial services companies or are in possession of banking licenses of their own. Thus, fraudsters seeking to ‘follow the cash’ now have many more avenues to fulfil their objectives.

While the financial services industry, by virtue of its highly regulated environment, has over the decades built up sophisticated control mechanisms, detection methodologies and risk management tools, the hybrids are generally yet to adapt themselves to the risks and the fast-evolving compliance landscape they now find themselves in.



Profile of the fraudster



In 97% of the cases in India, the internal employee is male (as against 79% globally).



S/he is aged between 31 to 40 years (61% of the respondents in India as against 42% globally).



S/he is a junior to mid-level manager (32% and 43% in India and 32% and 35% globally, respectively).

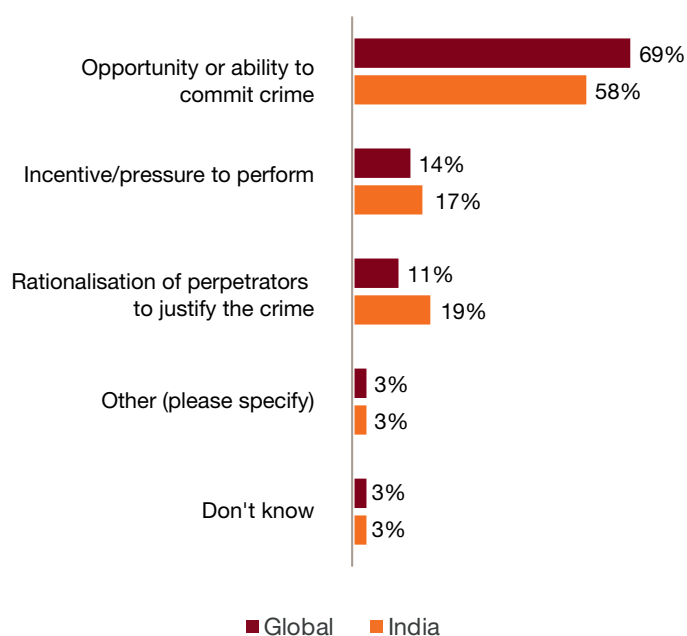


S/he is highly qualified/educated (at least a graduate or postgraduate) and reasonably experienced (having completed at least three years of service).



As per the survey results, 61% of the respondents in India believed that the main perpetrator in the most serious cases of economic crime was internal to the organisation, whereas only 16% considered the main perpetrator to be an external player, such as a vendor or a customer.

Which factor do you feel has contributed the most to economic crime committed by internal actors?



PwC India Speak

Dinesh Anand

Partner and Leader
Forensic Services
India



'Just like other criminals, fraudsters do not come with any distinct traits that can help us to identify them.

They can be working around us, above us, mingling with us in our day-to-day work life—and we may have no clue that we are involving ourselves in their malicious schemes and motives. This is why familiarising ourselves with the profile of a fraudster can prove to be a valuable training and awareness tool when it comes to safeguarding against fraud. In fact, the more we know and educate ourselves and others about the way fraudsters work, the better we can get at preventing fraudulent behaviour.'



External players

Only 16% of the Indian respondents believed that fraud could be perpetrated by external players, as compared to 41% globally. Out of these external players, Indian respondents believed that agents/intermediaries (40%) were most likely to commit fraud, followed by customers (30%).

Globally, most of the external players were customers or other external parties (25–28%).

Methods of detecting fraud

- In India, internal tip-off remains the most effective means to detect instances of economic crime, with 22% of the Indian respondents relying on the same. This was followed by detection by way of routine internal audits (13%), whistle-blower hotlines (12%) and suspicious transaction reporting (12%).
- Globally, the methods of fraud detection vary from the Indian results. The survey revealed that 14% of the respondents regarded suspicious transaction reporting as the most commonly used method to detect fraud, closely followed by routine internal audits (11%), internal tip-offs (11%) and detection by accident (11%).
- Today, an organisation's data runs into terabytes and the process and controls around data management are becoming increasingly complex and sophisticated. Hence, there is a growing need to focus on data analytics and periodic fraud risk management (FRM) as means of fraud detection. Currently, only 8% of the Indian respondents and 7% of the global respondents rely on data analytics, and 5% of the Indian and 8% of the global respondents, on FRM.



- In fact, 26% of the Indian respondents mentioned that they get FRM performed only annually. Further, 21% mentioned that they never had FRM done, while 20% were not aware of FRM being performed in their organisation. These results are in line with the global results.
- Approximately three-fourth of the total respondents in India and globally stated that they relied on internal resources to perform an investigation into incidents of potential fraud, which was followed by the engagement of a specialist forensic investigator and consulting with auditors and external legal advisors.



These findings point to potential weaknesses in internal controls, whereby these measures serve as check-box exercises rather than effective processes embedded into an organisation's culture. A crucial opportunity is now available to organisations to rethink their control structures and go back to fundamentals. Creating a culture of controls and risk awareness rather than one of ritualised activity, supplemented by zero tolerance for dishonest practices, can help insulate organisations from avoidable losses due to internal fraud.

Perception of law enforcement

Almost 50% of the respondents in India believed that law enforcement agencies in India are not adequately resourced and trained to investigate and prosecute economic crime, and only 25% believed the opposite to be true (the remaining respondents refrained from providing their views). These responses are similar to the global ones.

PwC India Speak

Sanganagouda Dhawalgi

Executive Director
Forensic Services
India



'We see law enforcement agencies in India coming up the curve in a big way. In the last few years, they have invested

extensively in technology, training and methodologies. We have had the opportunity to interact and work with many of these agencies and have been very impressed with their roadmaps and investments. The seeds sown now will no doubt mature into effective deterrents in times to come, and build confidence in the minds of citizens and corporates that our agencies are equipped to assist them when the need arises. However, there is still ground to be covered in this regard.'



New weapons of mass destruction



Deep penetration of technology in every facet of business has impacted the very nature of economic crime. In today's hyper-connected business ecosystem, crime has gone digital. So much so that while on the one hand, technology can be seen as aiding economic crime, it is simultaneously impeding it with the latest fraud detection tools and processes.

Further, given the global geopolitical climate and the rising threat of terrorism, the issues of money laundering and terrorist financing are increasingly on the radar of governments across the globe. In fact, global money-laundering transactions are estimated at 2–5% of the global GDP, or roughly 1–2 trillion USD annually, making this an area of safety and concern.

Cybercrime continues to rise

According to the survey findings, 56% of the Indian respondents felt that the risk of cybercrime had increased in the last two years. Cyber risk today encompasses more than just computers. Due to the rapid changes in technology and the advent of the Internet of things (IoT), there has been a sharp increase in attack activity involving interconnected devices in the cloud, including elements as diverse as cars and household devices.

Contrary to common perception, today, cybercrime is no longer an IT problem, but a fundamental business problem.

At a time when the scope, scale and sophistication of cyber risks faced by companies continue to rise, what's needed to combat this growing threat is not a digital strategy but a business strategy for the digital age—one more focussed on managing risks than on remediating incidents. For forward-thinking organisations, this is also where the opportunity lies.

Are board members paying enough attention to cyber readiness?

Surprisingly, only 45% of the companies in India reported that their board members inquired about the organisation's state of readiness to deal with cyber incidents. Further, 25% responded that they 'don't know', and 29% thought that board members either did not need this information or did not request for it. The tone at the top certainly needs to be more vigilant, and we expect numbers to go up significantly in the coming years. Organisations are expanding their businesses globally and have to face additional challenges when it comes to applying security policies similar to those at their base location in other countries because of local regulations and jurisdictions.

Impact of cybercrime

Only 16% of the Indian respondents affirmed that their organisation had been hit by cybercrime in the past two years. This is exactly half the global average of 32%.

While technology-related cyberattacks continue, the modus operandi is gradually becoming sophisticated. It is unfortunate that although there is greater recognition of the risk of cybercrime, most Indian companies remain oblivious to technology developments that can play an important role in preventing/writing off such events.

Financial loss due to cybercrime

In our survey, 66% of the respondents in India indicated that their organisation incurred a financial loss on account of cybercrime. More interestingly, 28% valued this loss at greater than 30 lakh INR. The figure could be much higher as 17% of the respondents said that they were unaware of whether or not they had suffered a financial loss.

Tracing the origins of cybercrime

While globally 51% of the respondents thought that cybercrime originates externally, in India, 43% believed that it has both internal and external origins. This suggests the greater risk of collusion resulting from weaker checks on employees and third-party due diligence.

PwC India Speak

Murali Talasila

Partner
Forensic Services
India



'With the proliferation of information on individuals and organisations across devices and social networks, there is a growing threat of misuse of such information. Intelligent minds can come up with innovative ways to combine open source intelligence, human intelligence, social media and network information, using deeper business acumen to break into organisations and business processes. Such threats can occur in the form of fraudulent financial transactions, business downtime, targeted attacks as well as organisation-wide shutdown of networks.'



Get cyber ready before it's too late



What are organisations doing to deal with the menace of cybercrime?



Is their governance and response plan adequately designed and implemented?



Are the first, second and third lines of defence in place to prevent, detect and respond to such untoward incidences?

Our survey revealed that 54% of the respondents in India had an incident response plan to deal with cyberattacks. However, only 42% stated that the plan was fully operational, and 18% were oblivious to whether or not their organisation had a response plan. Similarly, while 45% had identified a trained first responder (40% internal persons and 5% outsourced), a majority of the companies need to fill this gap.

Cyber readiness does not end with having incident response plans. Besides hiring trained technology and security professionals and the formulation of a security operations vertical, it involves setting up a process that integrates security measures across the entire ecosystem of an organisation and continuously monitors not only threats but also the incoming and outgoing activity across channels and networks.

Of the companies surveyed in India, 74% relied on their IT security specialist to double up as the first responder. Only 12% had a digital forensic investigator who acted as the first responder. This is an indication that, in most cases, companies

tend to identify the problem, plug the gap and move on. They do not focus on investigating and initiating legal proceedings. There are cases where lack of understanding of the process of evidence collection and preservation can weaken the cybercrime case when companies want to take the legal route. This becomes even more pertinent in cases of intellectual property (IP) theft and corporate espionage. Incident response and forensic teams have to integrate and work together, so that they are in a position to collect evidence before incident teams wipe it off as part of recovery procedures. Constant emphasis on laying down detailed standard operating procedures, continuous improvements and staying up-to-date with global technology trends will lead to greater success in defending against cyberattacks.

From crisis to opportunity

A cyber corporate crisis is one of the most complex and challenging issues an organisation can face. Cyber breaches require sophisticated communication and investigative strategies, including significant forensic and analytical capabilities that are executed with precision, agility and equanimity.

Although potentially daunting, ramping up preparedness has its silver lining: You can view it as an organisational stress test—one that can and should lead to improvements in your processes. In today's risk landscape, a company's degree of readiness to handle a cyber crisis can serve as a marker of competitive advantage and, ultimately, its survival.



Anti-money laundering (AML): Are you prepared to respond to the fast-changing regulatory environment?

Money laundering facilitates economic crime and nefarious activities such as corruption, terrorism, tax evasion, and drug and human trafficking. It can also seriously bruise an organisation's reputation and its bottom line.

Global money-laundering transactions are estimated at 2–5% of the global GDP,¹ or roughly 1–2 trillion USD annually. Yet, according to the United Nations Office on Drugs and Crime (UNODC), less than 1% of global illicit financial flows are currently seized by authorities.

Given the recent increase in terrorist attacks, governments across the globe are actively monitoring money laundering and terrorist financing.

As regulations become more complex and widen in scope, the cost of compliance continues to rise. Keeping up with regulatory developments, which can be fragmented and inconsistent across the globe, is an increasingly onerous task. According to new figures from WealthInsight, the global spending on AML compliance² is set to grow to more than 8 billion USD by 2017 (a compounded annual growth rate of almost 9%). But many institutions are balking at the idea of increasing their compliance spend—notwithstanding the fact that compliance failures have resulted in enforcement actions and large-scale penalties.

1) United Nations. (2011). Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes. United Nations Office on Drugs and Crime.
2) Data taken from <http://www.wealthinsight.com/>



Key findings in India

As compared to 74% of the financial institutions (FIs) globally, 56% in India have performed an AML/ combatting the financing of terrorism (CFT) risk assessment across their business and geographies. Globally, 6% of FIs considered this assessment to be unnecessary, but this number is 12% in India. However, 6% of Indian FIs reported that this was a focus area in the next 12 months.

With multiple regulatory enhancements driven by financial regulators in India with a focus on AML and CFT, FIs will undergo a paradigm shift in their regulatory and compliance regime. The Reserve Bank of India has released master circulars emphasising an AML compliance programme for all FIs. Further, the Black Money Act was passed in 2015 to combat tax evasion and money laundering. Trade-based money laundering has become rampant in the recent past, due to which FIs are now moving towards developing AML compliance programmes with a special focus on trade finance. Trade finance is now being viewed as a risk-prone area and it will be an important aspect for a risk assessment exercise at any FI.

Key challenges of complying with AML requirements in India

Three of the biggest challenges to effective AML compliance cited by financial industry firms are:





Heightened regulatory standards are driving a sharp increase in enforcement action. Our survey shows that the level of enforcement of AML and CFT measures has created challenges for even sophisticated FIs.

Factors that impede operationalising a holistic AML framework for FIs in India:



Rudimentary business models

Budgetary constraints



Lack of skilled and well-trained staff

Data inefficiency



Pace of regulatory changes



Detecting and deterring trade-based money laundering

Both globally and in India, increased customer due diligence requirements in industries targeted by regulators for greater scrutiny scored the highest at 64% and 70% respectively. The second choice is conducting a focussed periodic review of holistic activity for clients involved in high-risk businesses or jurisdictions. Globally, 43% respondents selected this, while in India, 40% opted for it. A majority of the respondents also selected conducting of specialised analytics to identify unusual trade practices and/or patterns consistent with undervaluation or over-invoicing of goods and services (40% and 33% globally and in India, respectively).

These findings suggest that trade-based money laundering is a concern in all economies and that a large number of FIs have implemented relevant controls to mitigate this risk. In India, the Indian Banks' Association (IBA) has released recommended scenarios or triggers for monitoring trade finance transactions in order to combat trade-based money laundering.

People and processes

Globally, 48% of the respondents claimed to have conducted local/regional/global training focussed on an aligned approach to compliance, and 44% stated they had hired additional compliance resources in regulation-specific roles such as AML/CFT, anti-bribery and corruption, and sanctions. In India as well, these were the two top choices at 47% and 40% of the respondents.

Further, there has been a sudden surge in the appointment of qualified and experienced staff for these roles in India. Most of the banks, both public and private, require their staff to hold accreditation in AML and a thorough understanding of dynamic subjects such as economic and trade sanctions. Apart from this, we see a lot of emphasis being placed on training employees periodically and equipping them with the right tools to communicate and disseminate regulatory updates. Regulators such as the Reserve Bank of India publish and distribute updates on the AML regime periodically.

Action points for organisations

PwC India Speak

Dhruv Chawla
Partner
Forensic Services
India



'A lot has been done but a lot more remains to be done. Installing a robust, up-to-date AML compliance programme—and embedding it effectively using people, processes and technology—can yield multiple business benefits, not just with respect to AML efforts, but also with other key global compliance functions, such as anti-bribery, export sanctions, fraud monitoring and response, and financial controls and investigations, thus potentially strengthening overall governance. According to the survey and consistent with our experience, one needs to keep one's finger on the regulatory pulse, lead the pack and not follow others, and learn from the mistakes of other financial institutions.'





Countering fraud

Business ethics and compliance programmes

88%

of the organisations surveyed in India have a formal business ethics and compliance programme

56%

of the organisations have seen an increase in their spend on compliance programmes and resources

61%

plan to increase their spend on compliance programmes in the next 24 months



A vast majority of the respondents (88%) were found to believe that their organisation had a formal business ethics and compliance programme in place. The responsibility, however, seems to be defined differently across organisations. While around 49% believed that the chief compliance officer was responsible for maintaining the business ethics and compliance programme in an organisation (as compared to 38% globally), human resources was the second most popular choice (at 17%), and the general counsel, the third (at 13%). A majority of the Indian respondents (82%) tended to believe that internal audit (IA) was the mechanism to ensure compliance with the programme. Management reporting (68%), whistle-blowing (58%) and external audit (35%) were the next three popular choices.

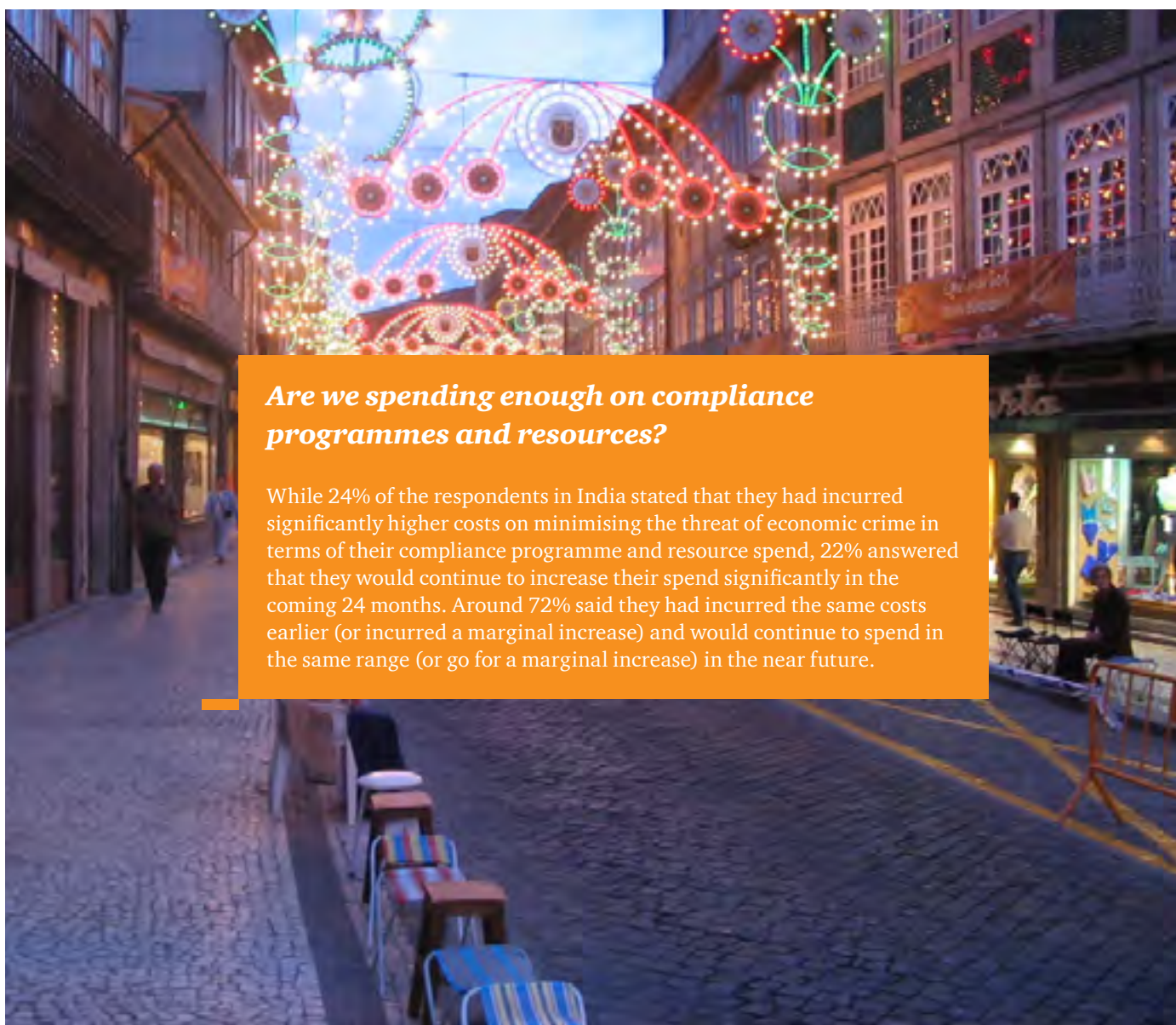
PwC India Speak

Geetu Singh

Partner
Forensic Services
India



'In our experience, forward-looking predictive analytics and real-time monitoring activities can constitute an effective line of defence against economic crime in the future. While audits—and, in particular, internal audits—are useful, they are often not adequately sophisticated or focussed on crime prevention. Additionally, the timing may not be conducive to preventing perpetration, resulting in losses by the time it is detected in an audit. We see more and more organisations today experimenting with data analytics and building the foundation for the future. But we in India are still at a relatively evolutionary stage with regard to the development and use of fraud-related analytics.'



Are we spending enough on compliance programmes and resources?

While 24% of the respondents in India stated that they had incurred significantly higher costs on minimising the threat of economic crime in terms of their compliance programme and resource spend, 22% answered that they would continue to increase their spend significantly in the coming 24 months. Around 72% said they had incurred the same costs earlier (or incurred a marginal increase) and would continue to spend in the same range (or go for a marginal increase) in the near future.



Key findings

- Although **94%** of the respondents agreed (or strongly agreed) that their organisation had a clear code of conduct and that their values were clearly understood, there was less clarity when they were probed for finer details.



Around **15%** were either unsure or did not agree that their leaders walked the talk.



Around **24%** were either unsure or did not agree that there was effective communication and training with regard to these policies.



Around **21%** were either unsure or did not agree that rewards were consistent and fair and that disciplinary procedures and penalties were consistently applied.

- While **58%** agreed that whistle-blowing serves as a mechanism to ensure compliance, **19%** feared retaliation and felt that feedback was not provided on a timely basis.

- When asked about their colleagues' perception of the leadership's response to corruption, the responses were mixed. However, **91%** of the respondents agreed that the leadership recognised the fact that bribery was not a legitimate practice.



19% were not sure whether they would let a transaction fail if bribery were the alternative.



15% did not resolutely back corporate guidelines.



25% were either unsure or believed that their leaders would not take a public stand against corruption.



19% did not expect, or were not clear about whether they wanted, their business partners to take a stand against corruption.

- Finally, **16%** of the respondents did not expect the government to take an unbiased approach to anti-corruption.

While bribery and corruption represent only one area of economic crime, they can serve as a key barometer of today's compliance trends. Our survey shows that **41%** of the companies who experienced an economic crime stated they had been asked to pay a bribe over the last 24 months.

PwC India Speak

Rahul Lalit

Partner
Forensic Services
India



'According to the survey results, bribery and corruption continue to impact the business environment in India. We also find that these issues are now discussed more openly by business partners. Be it an investment, divestment, new business relationship or other business situation, we see more due diligence activity around potential improper payments. Another positive development is more training on anti-bribery and corruption compliance. The heart of the matter is how to deal with the issues that arise when improper payments are made. Reporting these issues to regulators both in India and overseas is an extremely important process that cannot be undermined in any way.'





Last word

From crisis to opportunity

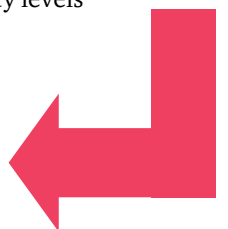
◀◀ Looking back



Dinesh Anand
Partner and Leader
Forensic Services
India

We sincerely thank our survey respondents for their forthright responses. In many ways, this survey presents the issues and challenges we face in our work and engagements every day. Looking back on the year gone by, here are some important observations:

- ◀ Corporate India continues to face an increasing onslaught of economic crime. A rising number of incidents, both within organisations and in the economy, clearly indicate that we are dealing with a problem that is endemic and has a significant magnitude.
- ◀ Perpetration methods have changed, become more sophisticated, and the modus operandi has also evolved. Losses incurred have increased from lakhs to crores, and from millions to tens of millions.
- ◀ Everyone is at risk and no one is immune. It is getting harder to predict where one can be hit from, as vulnerabilities exist everywhere.
- ◀ However, there have been many positive developments. Investments in countermeasures have started paying off, compliance programmes have come of age, regulations have become more stringent, and maturity levels related to handling of issues have increased.



Looking ahead

Gagan Puri

Partner
Forensic Services
India



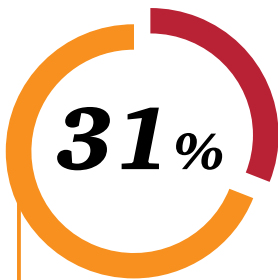
What lies ahead? Through discussions and interactions with our clients and the business community, we anticipate a greater impact on the methods used to perpetrate as well as mitigate economic crime. We mainly foresee that:

- ▶ New age crime will dominate all economic crime in the near future. Whether it is cybercrime, terrorist financing or technology-related fraud, the world will have to move quickly and nimbly in addressing and combatting these challenges.
- ▶ New age fraud will require new age countermeasures. Current risk management and compliance activities are in need of significant tailoring and modification in order to address the business environment of the future.
- ▶ Every crisis will need to be turned into an opportunity. Continuous improvement and constant evolution will become the cornerstones of a good compliance programme. Organisations can no longer play the victim; they really need to up the ante in their fight against economic crime.

Top-line facts



More than one in every four organisations in India are impacted by economic crime

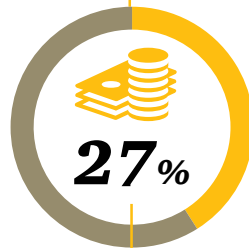


of the respondents in India have experienced economic crime in the last two years, as compared to 36% of the respondents across the globe

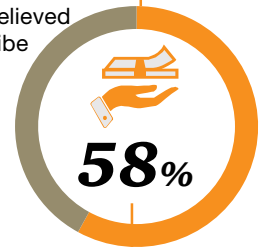
Bribery: A threat to expansion



of the organisations have lost an opportunity to a competitor which is believed to have paid a bribe



of the organisations in India have been asked to pay a bribe in the last 24 months



of the respondents strongly agreed that they would rather allow a business transaction to fail than pay a bribe



Profile of the fraudster in India

Middle management is now the main perpetrator of economic crime.



Male



Aged between 31 and 40 years



Has obtained a university degree



Has been with his employer for a period between three to five years



The typical perpetrator of fraud in India is:

Detecting fraud

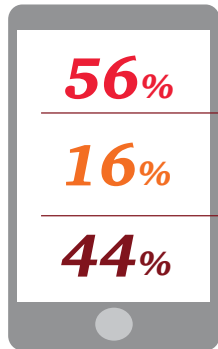


of the organisations have not conducted a fraud risk assessment in the last 24 months, while 20% do not know about it



have conducted this assessment annually, while 5% conduct it every 6 months

Cybercrime: A growing risk?



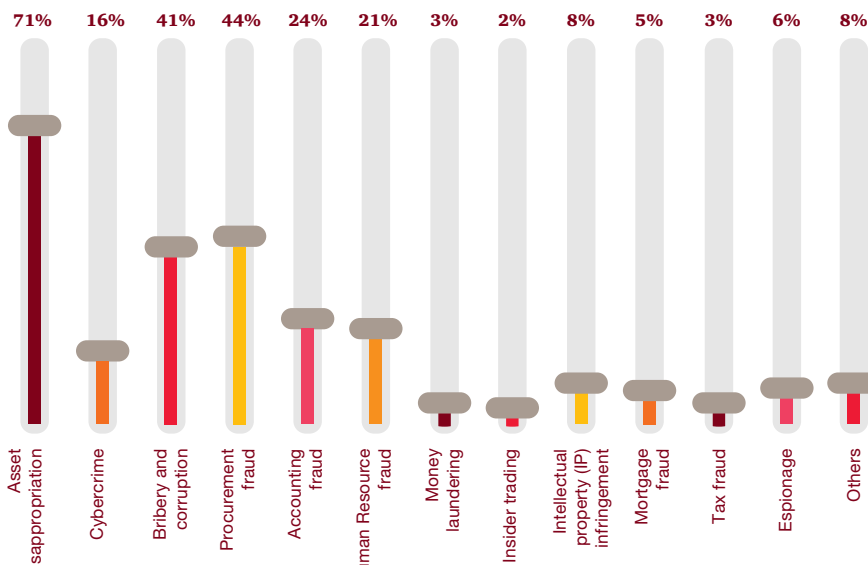
▶ of the Indian respondents have perceived an increased risk of cybercrime over the past 24 months

▶ of the organisations have been affected by cybercrime in the past 24 months

▶ of the respondents in India feel that local law enforcement agencies don't have the required skill and resources to investigate cybercrime, hacking incidents and malware-related fraud

Most common types of economic crimes

Asset misappropriation is most experienced type of economic crime by organisations in India in the last 24 months, followed by procurement frauds and bribery and corruption



Ethics and compliance



of the organisations in India have a formal business ethics and compliance programme



of the organisations have seen an increase in their spend on compliance programmes and resources



of the Indian respondents stated that their organisation had a clear code of conduct



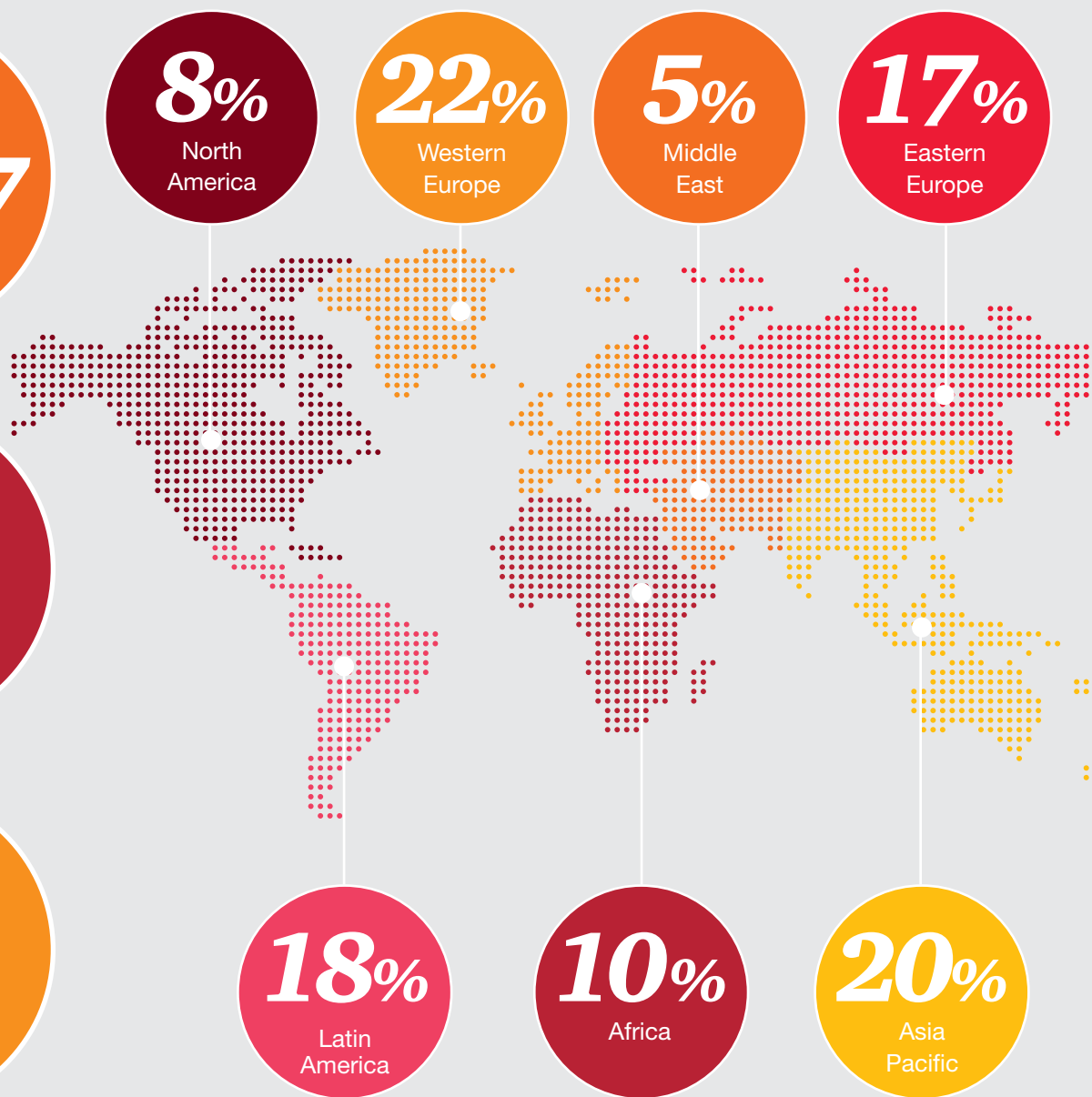
of the respondents indicated that their leaders did not walk the talk, 24% mentioned unclear communication and training, and 19% feared retaliation for reporting a violation

Global survey participation statistics

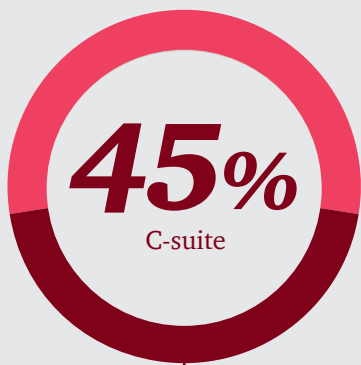
Participation statistics



Participation by region



Respondents



70%

of the respondents were managing finance, executive management, audit, compliance and risk management functions.

54%

of the respondents are employed by organisations with more than 1,000 employees, with

48%

of these participants having more than 10,000 employees.

37%

of the survey population represented publicly traded companies, and

59%

of the respondents were from multinational organisations.

Industry sectors



35%

Industrial



24%

Financial services



14%

Consumer



7%

Technology



6%

Professional services



13%

Other

Contact

Dinesh Anand

Partner and Leader

Forensic Services, India

Mobile: +91 9818267114

Email: dinesh.anand@in.pwc.com

Survey methodology

We conducted the Global Economic Crime Survey in India between July 2015 and February 2016. The findings of this survey report are based on senior executives' experiences related to economic crime. We obtained information from them on the different types of economic crime, their impact on the organisation (both in terms of financial loss and any collateral damage), the perpetrators of these crimes, the action taken by the organisation and the response to the crime.

The survey comprised six sections dealing with the following areas:

- Organisational profile
- Economic crime trends
- Technology
- Profile of the fraudster and economic crime detection methods
- Business ethics and compliance programmes
- Anti-money laundering and counter financing of terrorism

We'd be happy to offer an executive briefing on the survey to your organisation. For more information, please contact Dinesh Anand at dinesh.anand@in.pwc.com

About Forensic Services India

The PwC Forensic Services practice provides access to deep forensic capabilities across the globe. We offer forensic accounting, financial analysis and regulatory knowledge to companies faced with corporate investigations, litigation and regulatory enforcement challenges. As pioneers of forensic services in India, we also offer guidance and assistance with complex technology challenges.

Our team identifies and deals with a wide range of financial irregularities or fraud, misconduct and business disputes, and delivers clear, logical analysis and fact-finding reports. These solutions are facilitated by a variety of quantitative and qualitative techniques that isolate and analyse information derived from various cases.

About PwC


At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 2,08,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com


In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity in separate lines of service. Please see www.pwc.com/structure for further details.

 facebook.com/PwCIndia

 twitter.com/PwC_IN

 linkedin.com/company/pwc-india

 youtube.com/pwc