Reshaping the future of compliance with emerging technologies

Forensic & Integrity Services

ACFE
Association of Certified Fraud Examiners
Mumbai Chapter #160

EY
Building a better working world

Contents

Introduction 04

Foreword 05

Executive summary 06

Fraud and corruption risks in a technology driven era 08

RPA adoption in compliance at a nascent stage 12

Taking the next leap with AI and blockchain 14

Cyber risks rise with remote working 16

Prioritizing data privacy and data protection 20

The digital transformation of corporate compliance 24

In conclusion: reframing the future of compliance 27

About the survey 28

Introduction

The disruption from the COVID-19 pandemic brought a marked change within organizations as they dealt with restricted business operations, deviations in standard procedures and remote working. Technology emerged as an essential enabler to overcome the challenges faced and to foster agility in the modern workplace. The current wave of digital transformation engulfing corporate India is driving the use of emerging technologies in new ways and uncharted areas.

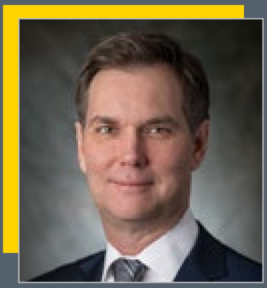
EY Forensic & Integrity Services and the Association of Certified Fraud Examiners (ACFE) Mumbai Chapter's latest report highlights that fraud, corruption, cybercrime, regulatory scrutiny and data privacy concerns have increased significantly over the last one year. These concerns have ushered in a new era of acceptance for the enhanced use of technology within anti-fraud, compliance and risk management frameworks. Consequentially, the challenges are also a catalyst for greater investments in technology. As per the report, 60% of the respondents said they plan to increase investments in forensic technology, encompassing tools, capabilities and people, to strengthen compliance and integrity frameworks.

The report shows that increased regulatory scrutiny has been the driving force, with 50% of respondents citing it as the key reason to use forensic technology. As enforcement action and regulatory oversight continues aggressively, organizations should harness the power of technology to meet regulatory expectations and maintain stakeholder trust. Emerging technologies such as Artificial Intelligence (AI), cyber forensics, Robotic Process Automation (RPA) and blockchain are expected to see significant momentum to establish data and metric led compliance programs.

Global organizations must manage numerous entities, with different organizational goals, omnipresent risks, data overload and multiple risk and compliance programs. Corporate resilience cannot be achieved overnight. Companies that will embrace change for an ethical and digital future, and follow appropriate strategic imperatives are likely to have a better chance of weathering crises and creating long term value. We would like to thank everyone who shared their viewpoint for this report and hope that it is beneficial.

Arpinder Singh

Global Markets and India Leader, Forensic & Integrity Services, EY
and President and Founder - ACFE Mumbai Chapter



Foreword

Change is inevitable. But the change forced upon us during the worldwide pandemic was nothing we expected. As this report from EY and the ACFE Mumbai Chapter points out, however, our colleagues from corporate India adjusted to this "new normal" admirably.

It is encouraging to see so many organizations within corporate India embracing technology and making the requisite investments to stay ahead. The pandemic demonstrated that, even though most of the world was on lockdown, cyber criminals and fraudsters did not take a day off. This report recognizes the hyperspeed changes in technology, and demonstrates what organizations are doing to prepare their workforces, their compliance programs, and their anti-fraud initiatives to embrace these changes.

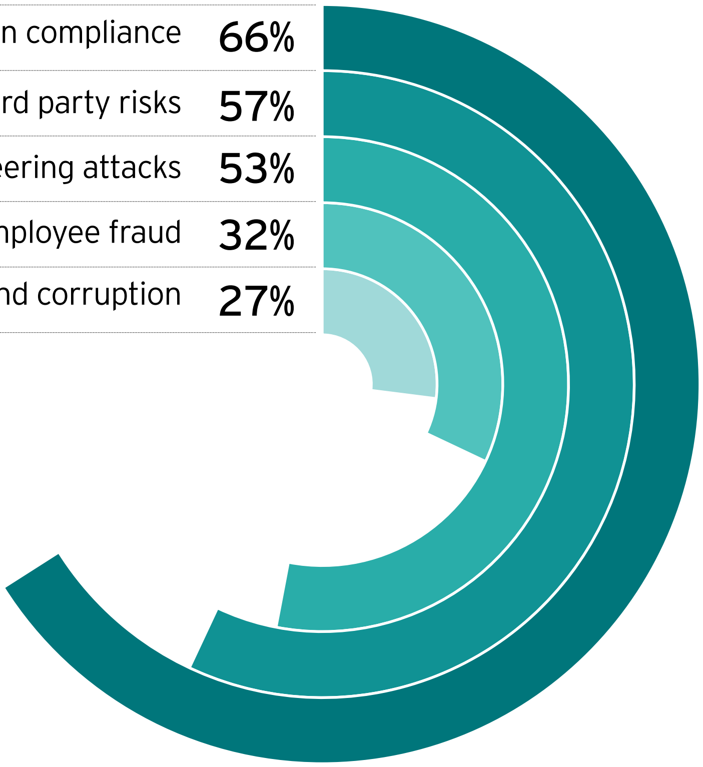
EY and the ACFE Mumbai Chapter have done an outstanding job in compiling this data that provides valuable insights on the state of compliance and anti-fraud technology within corporate India.

Bruce Dorris
President and CEO
ACFE

Executive summary

Corporate India's rising concerns in the last one year

Data privacy and data protection compliance	66%
Third party risks	57%
Cybercrime, ransomware, social engineering attacks	53%
Employee fraud	32%
Bribery and corruption	27%



Regulatory scrutiny driving increased investments in technology

60% plan to increase investments in forensic technology for compliance and integrity frameworks

32% state meeting regulatory expectations as one of the primary benefits for technology in compliance and anti-fraud frameworks

50% cite increased regulatory scrutiny as one of the key reasons to use forensic technology for compliance, risk and legal frameworks

42% said the level of concern around regulatory response has increased over the last one year

Innovative technologies are expected to be utilized frequently in compliance, risk and legal frameworks over the next two years

57%
AI

47%
Cyber forensics

42%
RPA

30%
Blockchain

Emerging industry trends

66%
are not using RPA based tools for compliance

50%
had cyber insurance, out of which 28% had an annual premium of over INR 20 lacs

40%
had a cyber breach, out of which 11% suffered a financial loss

41%
felt the biggest challenge in managing data protection and data privacy compliance was limited understanding of the relevant regulations in multiple jurisdictions

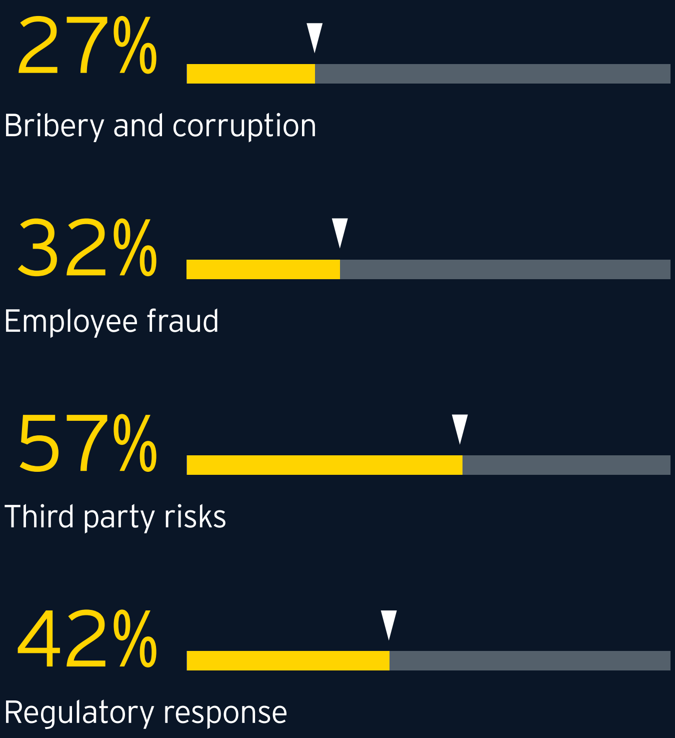
General Data Protection Regulation (GDPR) propelling changes in organizations

61%
said that Personally Identifiable Information (PII) saved was reassessed

59%
said they increased employee trainings on privacy and security

Fraud and corruption risks in a technology driven era

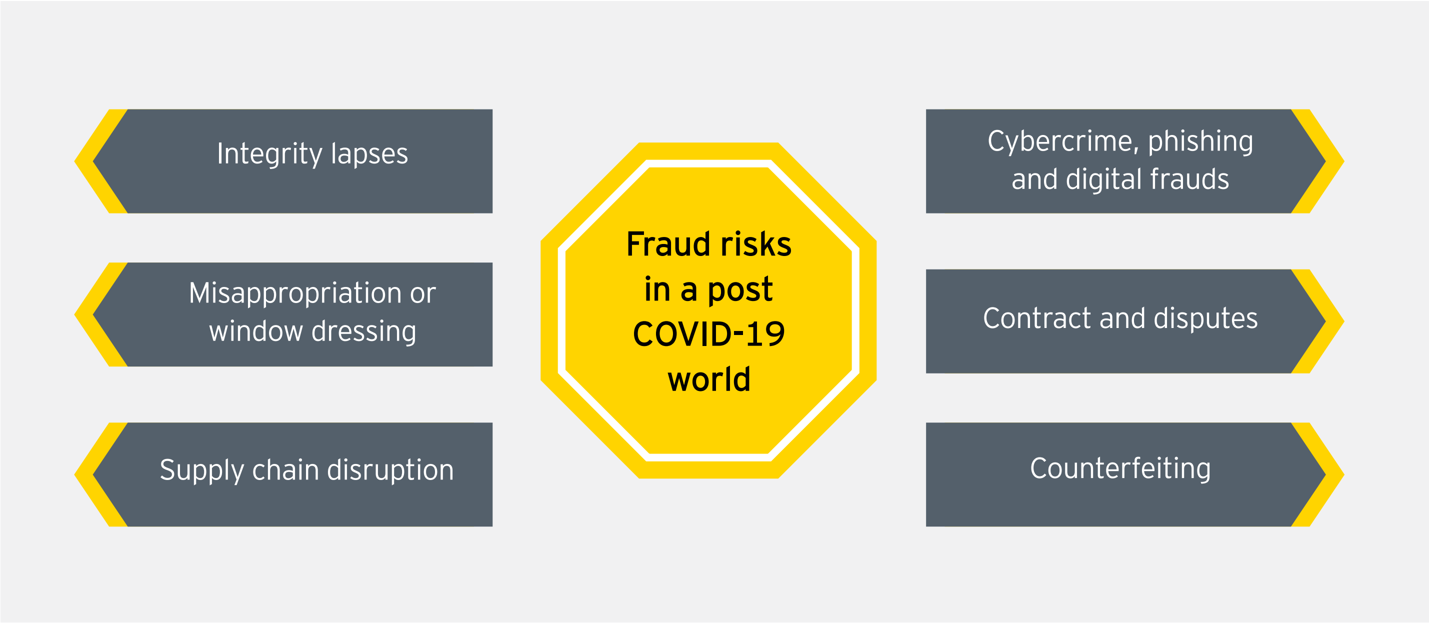
Increasing concerns for companies in the last one year



The spotlight on fraud, bribery, corruption and corporate misconduct issues have magnified in the last couple of years. One of the key reasons has been the enforcement of regulations in India (Companies (Amendment) Act, 2019, Fugitive Economic Offenders Act, 2018, Prevention of Corruption (Amendment) Act, 2018, Whistleblowing and Insider Trading Regulations by SEBI and The Companies (Auditor's Report) Order, 2020) and global laws including the Foreign Corrupt Practices Act (FCPA) and UK Bribery Act. These have led to tighter norms and increased scrutiny of corporate India and its business practices. Today, management and board of directors are more responsible and accountable than ever before for the action of the companies, staff, third parties and other stakeholders.

This risk factor has heightened during the COVID-19 pandemic. There was widespread disruption, business pressure, remote working and a generally unfavorable economic climate. The survey highlights that concerns around bribery, corruption, fraud (third party, employee) and regulatory response have increased over the last one year.

The nationwide lockdown had an adverse impact on all business functions, including compliance, risk, legal and investigations that found it difficult to manage controls, standard operating procedures (SOPs) and processes. Technology emerged as the driving force to maintain business continuity. It was observed that companies at the higher end of the maturity curve in technology adoption were able to manage the crisis relatively better than many others. From digital interviews, to remote investigations, use of data analytics, AI and machine learning - compliance and risk teams could fine-tune their approach to deal with imminent threats, enhance fraud detection and deterrence, and address regulatory requirements.



Fraud risks in a post COVID-19 world

Integrity lapses

Misappropriation or window dressing

Supply chain disruption

Cybercrime, phishing and digital frauds

Contract and disputes

Counterfeiting

Accelerating investments in innovative technologies to counter growing risks

60%

plan to increase investments in forensic technology for compliance frameworks

Key reasons to use technology in compliance

50%

Increased regulatory scrutiny

49%

Greater cost efficiency in the fraud risk management process

40%

Rising fraud risks

37%

Recent incident of fraud or non-compliance

According to the survey, 60% of the respondents said they planned to increase investments in forensic technology for compliance frameworks (tools, capabilities and people). A critical success factor here would be for companies to minimize any potential disconnect between the developers and the end users. Another important consideration here is to have this integrated as part of their organization's overarching digital transformation journey, and not a siloed or disparate digitization plan.

Fraud can be committed in a variety of ways. For example, digitally stored company info can be compromised if:

- Sensitive data gets uploaded to the "cloud"
- Company information is emailed to personal accounts or unauthorized individuals
- Sensitive documents are saved on a smartphone
- Information is shared through social media

It is essential to safeguard confidential company information, so it is not shared externally or misused. For instance, monitoring technology that prompts a notification when company data is leaving the office network, or when it is shared online, is readily available. Organizations should consider collaborating with cyber forensic providers for threat hunt, network monitoring, vulnerability assessment and penetration testing (VAPT), red teaming and reconfiguring Security Operations Center (SOC) solutions including behavior-based security information and event management (SIEM) to identify threats at an early stage.

Maximizing the benefits of technology for compliance

71%

cite early risk detection as the main benefit of using forensic technology in compliance, risk and legal functions

32%

said meeting regulatory expectations

Leading organizations are moving from traditional rule-book methodologies of compliance management to web-based tools with business intelligence (BI) dashboards and AI enabled mobile based chat bots. There is a surge in SOP management tools development using cutting edge technologies and the demand will continue to exist even post COVID-19.

According to the survey, use of emerging technology would improve companies' overall compliance and risk strategy in the form of early risk detection. Other key benefits include lowered dependence on manual processes (62%) and enhanced risk assessment processes (59%). 52% said that they would have an improved response time investigation, 43% said there would be increased business transparency and 40% said there would be an end-to-end compliance management. These are all critical areas especially as traditional controls and fraud detection mechanisms may not be suitable in today's age. Increased disruption and new risks may render controls weaker with many people still working from home.

Technology in compliance and investigations

An advanced analytics program can be fruitful in deriving maximum value from data. In many cases, the sample data analytic techniques applied in reactive investigations are used for proactive monitoring programs. These include AI techniques such as topic modelling, linguistic analysis, statistical analysis and rule-based descriptive tests. Behavioral analytics and social network analysis are used more extensively in continuous monitoring. They help to identify patterns of unusual activities and hidden relationships, and to predict misconduct.

- Ability to demonstrate plans with help of technology helps companies to mitigate future litigation
- Enables discovery and classification of sensitive data as per regulations
- Driving increased transparency and better governance
- Enables companies to establish mature compliance programs

Case study 1

A leading US conglomerate used a Software as a service (SaaS) model to identify procurement and expense anomalies. The objective was to perform analytics related to bribery, corruption and Foreign Corrupt Practices Act (FCPA), accounts payable (AP) and travel and expenses (T&E) to identify red flags, usually difficult and time consuming to find through manual reviews.

The process involved integrating data from multiple sources into a unified model and performing analytics in the Purchase-to-Pay (P2P) and T&E areas to identify high risk vendors and employees. The technology assisted platform was also used to detect certain suspicious transactions, eliminated "sampling" and helped in continuous monitoring. Integrated case management also helped create pertinent cases. The results helped in effective decisions making and risk mitigation.

Harnessing the power of technology in a regulatory environment

From using Big data for real time reporting, to using AI for identifying and mitigating cases of fraudulent or irregular transactions, organizations should explore adopting innovative ways to address regulatory compliance using technology. The key areas where legal technology can be leveraged are document reviews, contract management, workflow tools, e-discovery, legal chatbots, online marketplaces, cloud-based databases and data security.

From a governance, risk and compliance (GRC) standpoint, technology can be used in the following key areas:

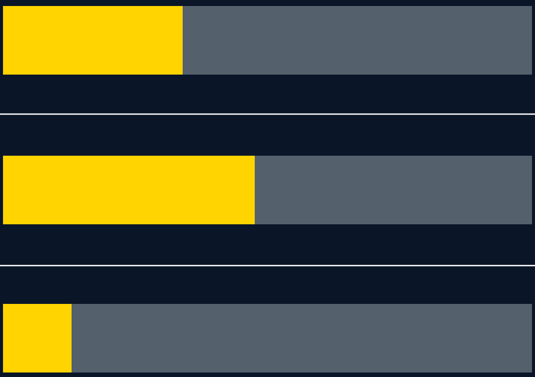
01 **Deeper layers of identity –** going above and beyond traditional security layers. This would also mean implementing state of the art identification mechanisms such as biometric authentication, mobile identity and risk intelligence patterns by looking at spend patterns or credit reports, and bank identities.

02 **Know your criminal –** building a cyber defense framework, which can potentially eliminate threats such as viruses, ransomware, phishing and other digital hazards

03 **Know your customer (KYC) –** complying with anti-money laundering laws and performing identity verification in the financial services sector

04 **Early Warning Systems (EWS) –** managing voluminous logs, automating analysis, workflow-based review process and maintaining traceability in the life sciences sector

RPA adoption in compliance at a nascent stage



33% state RPA as one the key technologies driving digital transformation within compliance, risk and legal functions

66% are not using RPA based tools for compliance

12% had developed a proprietary tool

Even though there has been an increase of using automation to remove manual processes across verticals and industries, companies are yet to adopt RPA to optimize their compliance frameworks. As data increases exponentially and processes become complex, companies need to adopt RPA in their overall risk framework, covering audit, controls and security.

It can become an essential element of companies' operations, streamlining and aligning several processes that are typically time and resource intensive, and difficult to error-proof.

RPA: an enabler for smarter compliance strategies

Areas where companies are planning to use RPA

46%

Workflow management

45%

Collect data from different sources

38%

Vendor due diligence and compliance reporting

33%

Customer due diligence

RPA can be utilized in areas ranging from monitoring, evidence collection, evaluation of controls and reporting, GRC enablement, application security enforcement, digital identity or access, data identification and protection and software security. Organizations with industry standard processes and SOPs can turn highly efficient as defined implementation of RPA is relatively easier. The benefits from RPA would include:

- Process modifications
- Baselining, testing and reporting of controls
- Governance framework enablement and extension
- Threat and vulnerability management that may not be streamlined or updated for years.

According to the survey, only 22% used a licensed tool from a vendor, while only 12% have developed a proprietary tool.

Practical applications of RPA

Fraud monitoring: comprehensive automation of business functions that are vulnerable to fraud, enhanced regulatory compliance, new insights on emerging areas of risk and generation of real time reports

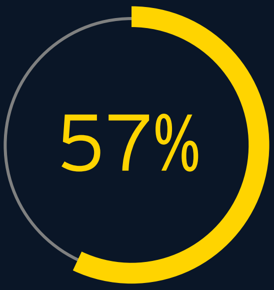
AML compliance: performing reviews on accounts, processing large data volumes, facilitating unsupervised learning on broad data access to eliminate false positives

Customer identification programs: validating internal systems and customer data aggregation to generate the customer KYC report, identifying and verifying data and conducting background checks

Case study 2

A consumer goods company integrated RPA within its compliance and risk framework with the objective to mitigate procurement fraud, involving potential conflict of interest (COI) with vendors. A bot was created for the procurement approval process, and filtered cases with potential COI were sent for stakeholder approval. Based on approval or rejection, the purchase order was updated in the relevant systems. This approval process identified potential COI cases for vendors and employees. Alerts were also sent to the management for unapproved vendors, which streamlined the due diligence for vendor on-boarding processes.

Taking the next leap with AI and blockchain



expect AI to be used regularly in compliance, risk and legal frameworks over the next two years

Utilizing the potential of AI

The Information Revolution has utilized the true potential of AI as it emerges as a game changer for organizations with bots and algorithms, bringing efficiency into processes. AI has the potential to discover new and unique trends and patterns from large data sets. There has been rapid growth in the intelligence of AI led machines over the last few years that are now capable of analysing documents, digitization and retrieving information.

AI can assist in carrying out compliance efforts, monitoring, and tracking external cyber threats. Risk, compliance and legal departments can harness the benefits of AI in the following areas:

Compliance Intelligence

The power of AI and Natural language processing (NLP) can aid compliance teams in reviewing contracts. NLP enables computers to understand human language, both text and speech which helps in categorizing data, measuring sentiment and other parameters. It therefore provides a platform to translate compliance and regulatory documents to structured set of rules so that the reviewing tasks can be automated. Machine learning analyses and understands unstructured data with help of algorithms which are capable of self -learning.

Risk Intelligence

AI along with Big Data and public and private databases can assist organizations perform KYC procedures and continuously monitor to predict future risks. The Risk Intelligence approach is expected to shift from a check in the box to a risk prevention strategy.

Legal Intelligence

AI can transform the way the legal teams review, compare and search documents. AI and NLP enable organizations to build a database, like a digital library of documents. AI enabled libraries can be searched by asking simple questions, providing similar documents and be sorted based on the type of contracts. The access to such a digital library can likely reduce more than 50% of the efforts for legal teams.

The case of ethical AI

One of the key questions increasingly faced by companies has been the ethical use of AI. This means, what if there is an unconscious bias in the algorithm? What if there are errors or defective design or even malicious intent? Who owns, uses, analyses, or disposes the data with the company? What if there is a data or cyber breach? Who is responsible for data in multi-party collaboration projects?

Poor use of data can be damaging for organizations from a reputational, legal and financial standpoint. AI led data management processes are under the spotlight these days, especially with respect to discrimination, data privacy, including having the "right to be forgotten" and possible misuse of customer data. With laws getting tighter and prosecutions rising – the accountability is higher than ever before. Additionally, it can become a challenge for companies as it could lead to drained resources, time and effort, and inefficient operations. Companies must therefore maintain responsible management and governance of data, set up processes to risk assess from concept to the design stage as projects move forward, and have continuous checks done, including sign offs from privacy, security or legal departments. Driving transparency and making investments in people can pave the way for an ethical future.

Harnessing the power of blockchain

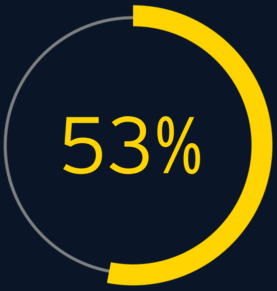
30%

expect blockchain to be used regularly in compliance, risk and legal frameworks over the next two years

The pandemic has accelerated organizations' digital transformation drive in many areas, including the use of blockchain or distributed ledger technology. The global blockchain market size is set to grow exponentially. Risk, legal and compliance departments can effectively use in several areas, for example identifying counterfeit drugs in the pharmaceutical industry to and bringing transparency and trust across the chain in the financial services sector.

The use of blockchain powered solutions in risk, legal and compliance is expected to rise further with many companies adopting it to establish chain of custody, ensure data privacy and enable a clear evidence for forensic investigations. Rising cybercrime and digital threats will further give an impetus to the use of blockchain as digital evidence is key for investigations.

Cyber risks rise with remote working



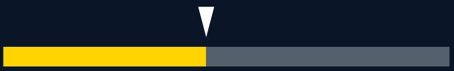
state that cybercrime, ransomware and social engineering (spoofing, phishing) risks have increased over the last one year

The COVID-19 pandemic led to a massive and sudden surge in work from home.

Employees worked outside the company network, many were able to open websites or download content or applications that they could not usually access at work. Unsecured websites, software exposures and lack of cyber awareness among employee saw cybercriminals exploiting organizational vulnerabilities.

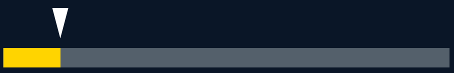
Cybercrime and ransomware attacks see an uptick

40%



reported a cyber breach in their organization over the last one year

11%



reported a financial loss as a result of the cyber breach

Over 50% of the respondents said that cybercrime, ransomware and social engineering (spoofing, phishing) risks have increased over the last one year. Cybercriminals are using malicious apps or software, delivered as an email attachment or link, to infect systems and networks. Critical company information is usually held as ransom, to be released after payment through bitcoins. The survey noted that about 40% of the respondents reported a cyber breach over the last one year. In 11% of the cases, there was a financial loss, which in case of large corporations can easily be to the tune of millions of dollars.

According to the survey, 39% of the respondents said that insider threats, including theft, manipulation or destruction of data have increased in the last one year. Insider threats are equally dangerous as external threats. Organizations should embrace digital transformation to strengthen the virtual infrastructure, develop strong monitoring frameworks, run diagnostics scans, establish incident response strategies and raise awareness among all stakeholders. Organizations must prepare for future scenarios that may impact business continuity by devising ways to respond to an information security incident effectively and dealing with the aftermath of a potential security breach.

Evolving trends in cybercrime in corporate India

Regulatory compliance and self-reporting of cyber breaches

52%

state that incidents of a cyber breach are disclosed to both internal and external stakeholders

Boards and CXOs must plan an adequate cybersecurity posture and accompanying administrative, technical and physical security controls, including reporting of breaches. Most countries now put the legal onus on companies to notify data protection authorities of certain data breaches. The survey notes that only half of the respondents disclosed a cyber breach to both internal and external stakeholders. Worryingly, 38% informed only internal stakeholders, while 9% did not report at all.

According to the GDPR ((as mentioned in Art. 33), all companies that deal with the data of EU citizens must report a notification of a personal data breach to the supervisory authority. Similarly, the Reserve Bank of India (RBI) mandates as part of the Annexure 3 to the circular on Cyber Security Framework in Banks[1], that breaches have to be reported through a security incident reporting (SIR) to the regulator within two to six hours.

Regulatory watchdogs, including the Indian Computer Emergency Response Team (CERT-In) mandate that companies, service providers and intermediaries should disclose and communicate to employees and customers, what data has been exposed, particularly in the case of PII or PHI.

Cyber insurance to protect business critical assets

50%

state having cyber insurance

28%

have taken policies with the annual premium of over INR 20 lacs

35%

are considering taking a cyber insurance policy

With the rise of such threats and attacks, companies have also started taking larger cyber insurance policies to safeguard their data. Known as cyber risk insurance or cyber liability insurance coverage (CLIC), companies are taking proactive steps to mitigate the risk and protect assets and reputation, but most of all, recover monetarily after a data or security breach[2]. The coverage of the cyber insurance typically varies – including but not limited to forensic investigation, business loss, costs for data breach notifications and legal expenses including (at times) the cost of paying ransom to attackers. Cyber insurance is becoming an absolute necessity and it helps companies salvage the business in the event of a data or a security breach.

[1] https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF

[2] https://www.theweek.in/news/biz-tech/2020/10/06/rise-in-ransomware-hacking-makes-india-the-second-most-attacked-country-globally.html#:~:text=While%20ransomware%20attacks%20increased%20by,Sri%20Lanka%2C%20Russia%20and%20Turkey

Social media risks

50%

cite early risk detection as the main benefit of using forensic technology in compliance, risk and legal functions

The survey observed that 52% of the respondents stated that risks arising from social media have risen in the last one year. These platforms are used extensively to connect with personal and professional networks. However, they are increasingly being exploited by cybercriminals to attack unsuspecting individuals using adverts, sharing buttons and plug-ins. In addition, companies may be exposed to risks around violation of Intellectual Property (IP) including circulation of illegal materials, misuse of trademarks and design or patent violation. Setting same passwords across different social media platforms and hackers selling the details on the dark web can be viewed as one of the weakest links. Hackers are stealing and selling personal information and taking control of personal devices to gain privileged access to company's network.

> "Cybersecurity must be enabled as a business culture within the organizations, moving from the data center to the boardroom.
>
> Harshavardhan Godugula
> Partner, Forensic & Integrity Services

Defending the enterprise – how can forensic technology battle cyber risks?

58%

cite growing cybercrime and ransomware risks as the main reason to use forensic technology for compliance, risk and legal frameworks

47%

state cyber forensics as one of the key technologies that are expected to be used regularly in compliance, risk and legal frameworks over the next two years

New forms of cyber-attacks such as business email compromise, phishing, next-gen ransomwares, cyber honey traps, cyber bullying and AI powered attacks are emerging rapidly. Cybersecurity must be enabled as a business culture within the organizations, moving from the data center to the boardroom.

Organizations need a strong defense "always" - an attacker needs to get lucky only once. A successful cyberattack on an unprepared business could cause irreparable damage for years. This can be in terms of data loss (confidential or proprietary), financial impact, brand erosion, customer loyalty and employee morale. With remote working still pervasive, this adaption to a personal setting as compared to a work setting leads to a general decrease in risk awareness.

Installing anti-virus software on endpoints is no longer enough to prevent attacks. As cyber weapons become destructive, organizations are struggling to identify and mitigate risks, both cyber and privacy related. The most valuable information for cyber criminals PII, passwords, financial data, PHI and intellectual property (IP) data. Initially, the purpose was to cause disruption, it has now evolved to a form of "corporate virtual kidnapping". Companies are held to a ransom till a payment (usually in the form of bitcoins) is made to the cybercriminals.

Compliance and technology teams will have to implement a cyber risk management strategy to help identify the threats to their organization. Developing a risk treatment plan can help address the risks and build the correct defenses in place. This reduces the threats from cyber-attacks. Complying with certain regulations as part of the cyber risk strategy will help organization's avoid hefty fines that can be given for non-compliance.

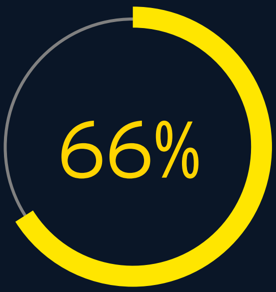
Dawn of the "compliance technologist"

The role of a compliance officer has progressed, and even more so during the pandemic. There has been a concerted shift to embrace technology, understand its practical and business implications and leverage it effectively. The new age compliance officer is expected to further transform into a "compliance technologist", recognizing the crucial areas where technology can be deployed. Innovation will be at the core of process improvements, information security, risk assessments and continuous monitoring. The convergence of compliance and technology cannot only enable a sharper approach to risk mitigation, but also become instrumental for greater regulatory observance.

Case study 3

A global firm witnessed a ransomware attack which rendered most of their systems unusable. While traditional endpoint protection tools were deployed, the company's IT team faced several challenges keeping them patched and up to date. The company sought the expertise of external forensic consultants to identify the source of the ransomware, remediate the systems back to their original state and assist in data recovery. A resiliency program was implemented, with detailed outlining of vision, mission, operating model, role and responsibilities, and SMART KPIs. A cadence program was also put in place for regular asset discovery and identification, and to ensure that unattended systems are not present. Along with this, it became imperative to identify end of life or end of support systems (obsolescence) and implement adequate security controls, along with enhancing the capabilities of existing security tools such as SIEM, anti-virus and endpoint detection and response (EDR).

Prioritizing data privacy and data protection

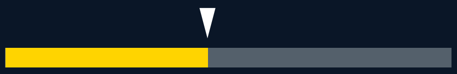


said that the level of concern around data privacy and data protection compliance has increased over the last one year

Companies are facing numerous challenges in protecting their data and making sure they comply with privacy laws. Two third of the respondents surveyed said that the level of concern around data privacy and data protection compliance has increased over the last one year. Data and technology come with its own set of risks which can have a significant impact on businesses. These are triggered in the form of human error, bias, faulty algorithm design, poor quality data or malicious insiders.

Adherence with global and local regulations

41%



said limited understanding of the relevant regulations in multiple jurisdictions is the biggest challenge in managing data protection and data privacy compliance

37%

were aware that their company's data (which may include personal data) is stored within Indian borders

Rising data privacy and protection concerns have led to new regulations around the world such as EU's GDPR and CCPA in the US. These stringent regulations have intensified the task of compliance, legal and technology teams. Non-compliance can prove to be detrimental to the business, potentially leading to hefty fines, reputational damage or shutdown of operations. Violations originate from outside the organization as much as from inside. The survey noted gaps in processes that would require addressal. Only 39% of the respondents are conducting compliance audits of third parties that handle personal data. Only half of the respondents stated that have a data privacy strategy that addresses all the requirements of global and local data privacy laws.

Areas where investments were made to ensure compliance with GDPR and the upcoming Indian Data Protection Bill

55%

System upgrades

41%

New technology

There has been an increase in investment in terms of knowledge, infrastructure and talent. 45% said they have ramped up information and data governance frameworks and 59% increased employee trainings on privacy and security post GDPR. Organizations that comply with the regulation requirements will build consumer trust and stand out from their competitors. Technologies such RPA and blockchain can enable businesses becoming compliant with data privacy and safety regulations standards. They can also improve oversight and compliance process accuracy.

Level of consumer control and cognizance

27%

have made investments to revamp consumer policies

66%

state explicit consent is taken from an individual in a clear and concise manner for all data processing activities

46%

state that a regularly updated and periodically audited data retention policy and process exists, which allows companies to delete data that is no longer needed for the purpose for which it was collected

Privacy and security are converging with an aim to protect private data as the common goal. Security measures need to go beyond fencing private data because anyone with access to large amounts of data, albeit considered non-private, can gain access to private information with the aid of AI and analytics technologies.

The survey highlights that many organizations are still struggling to keep customers at the heart of their data privacy and protection strategy. Only 27% have made investments to revamp consumer policies, and 41% have a provision to enable a data subject's (an individual whose personal data is with the organization) request to clear their personal data from their company's systems. On a positive note, 61% of the respondents said they re-assessed PII saved with the organization.

In India, The Information Technology Act, 2000 (IT Act), detailed the scope of access a consumer or individual might have on data stored electronically – this was augmented by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under Section 43A of the IT Act, which put in place further guidelines regarding data collection and disclosure – on the lines of GDPR. It is expected that the Personal Data Protection Bill (PDPB) 2019 will become an act in the coming months – and Indian consumers will have the legal right to obtain, erase and migrate data, and more importantly, raise grievances. The PDPB is expected to serve as a blueprint to define more robust and comprehensive data protection laws. It would be interesting to see how companies ramp up and transform their security and privacy models after this important development.

> “
>
> Privacy and security are converging with an aim to protect private data as the common goal.
>
> Ranjeeth Bellary
> Associate Partner, Forensic & Integrity Services

Data breach management: implementation and challenges

16%

said the organization does not make any provision for data breach management

21%

said their organization does not have a Data Privacy team

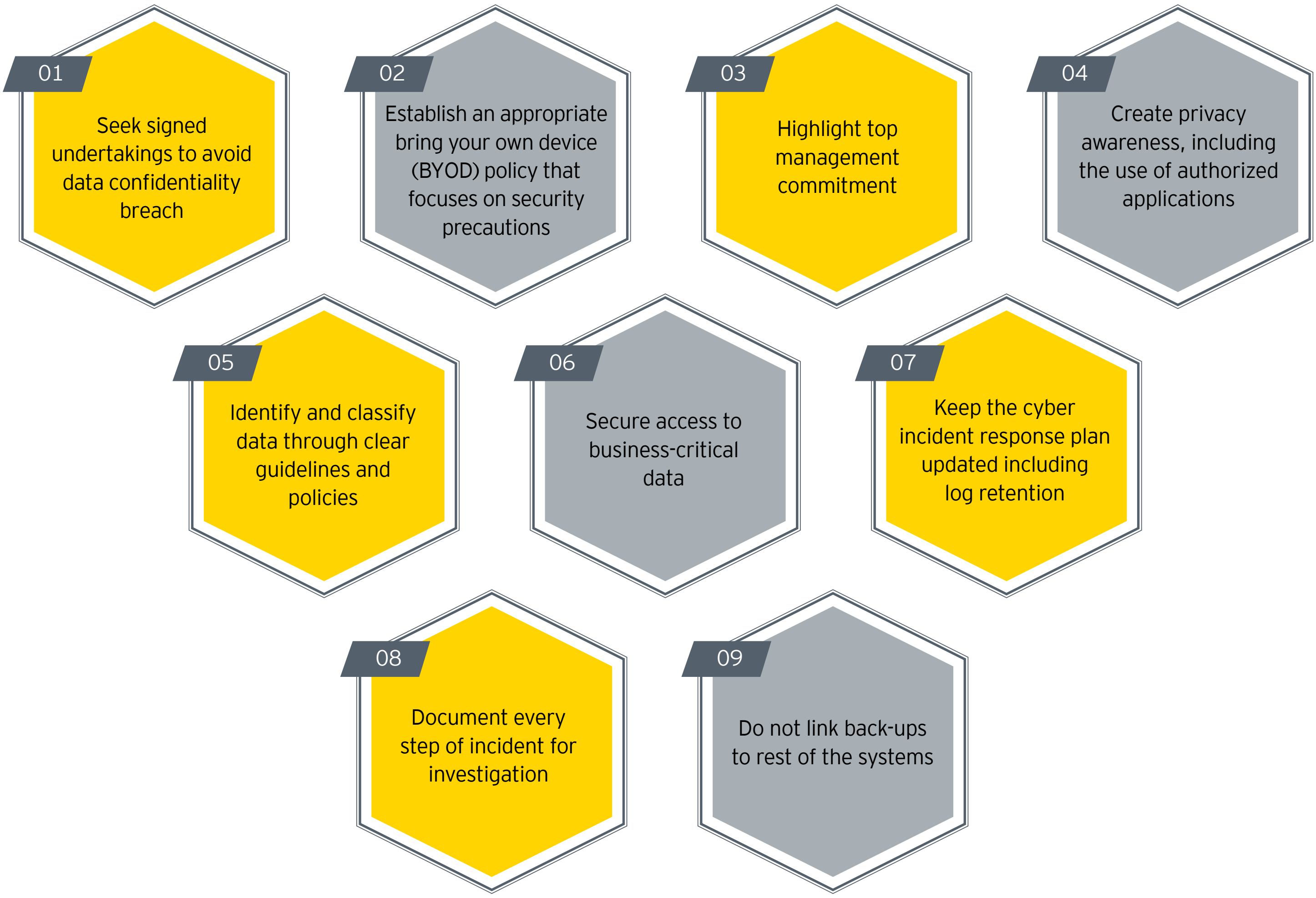
50%

did not have a Data Protection Officer

2020 saw some mega data breaches and ransomware attacks. CISOs and CTOs are realizing that merely investing in security platforms and third-party cybersecurity teams is not the answer. As enterprises awaken to the threats to internal and customer data, it's important to formulate and action a unified Forensics strategy to prepare for the inevitable. According to the survey, 16% said their organization does not make any provision for data breach management. On the other hand, 21% said their organization does not have a Data Privacy team; 50% did not have a Data Protection Officer.

Organizations should take steps to proactively assemble breach response team that combines internal stakeholders and external resources so they can be prepared in the event of a breach. A cybercrime investigation led by forensic specialists can uncover the details of how the breach occurred, data, systems and networks that are compromised, and who is responsible. Forensic technology led tools and platforms can be deployed to collect and preserve the evidence, analyze the data, restoration and remediation.

Leading practices for cyber and data breach investigations



01 Seek signed undertakings to avoid data confidentiality breach

02 Establish an appropriate bring your own device (BYOD) policy that focuses on security precautions

03 Highlight top management commitment

04 Create privacy awareness, including the use of authorized applications

05 Identify and classify data through clear guidelines and policies

06 Secure access to business-critical data

07 Keep the cyber incident response plan updated including log retention

08 Document every step of incident for investigation

09 Do not link back-ups to rest of the systems

38%

have an unclear understanding of data involved (where it is and who has access to it)

Breach response teams should be empowered to take action on data privacy and information governance. This starts with data discovery across all data - structured (e.g., ERP), unstructured (e.g., email) and semi-structured (e.g., CRM) to see what PII information is stored in the organization and with whom. However, the survey states that 38% of the respondents have an unclear understanding of data involved (where it is and who has access to it). This can pose a significant problem from a regulatory as well as operational standpoint.

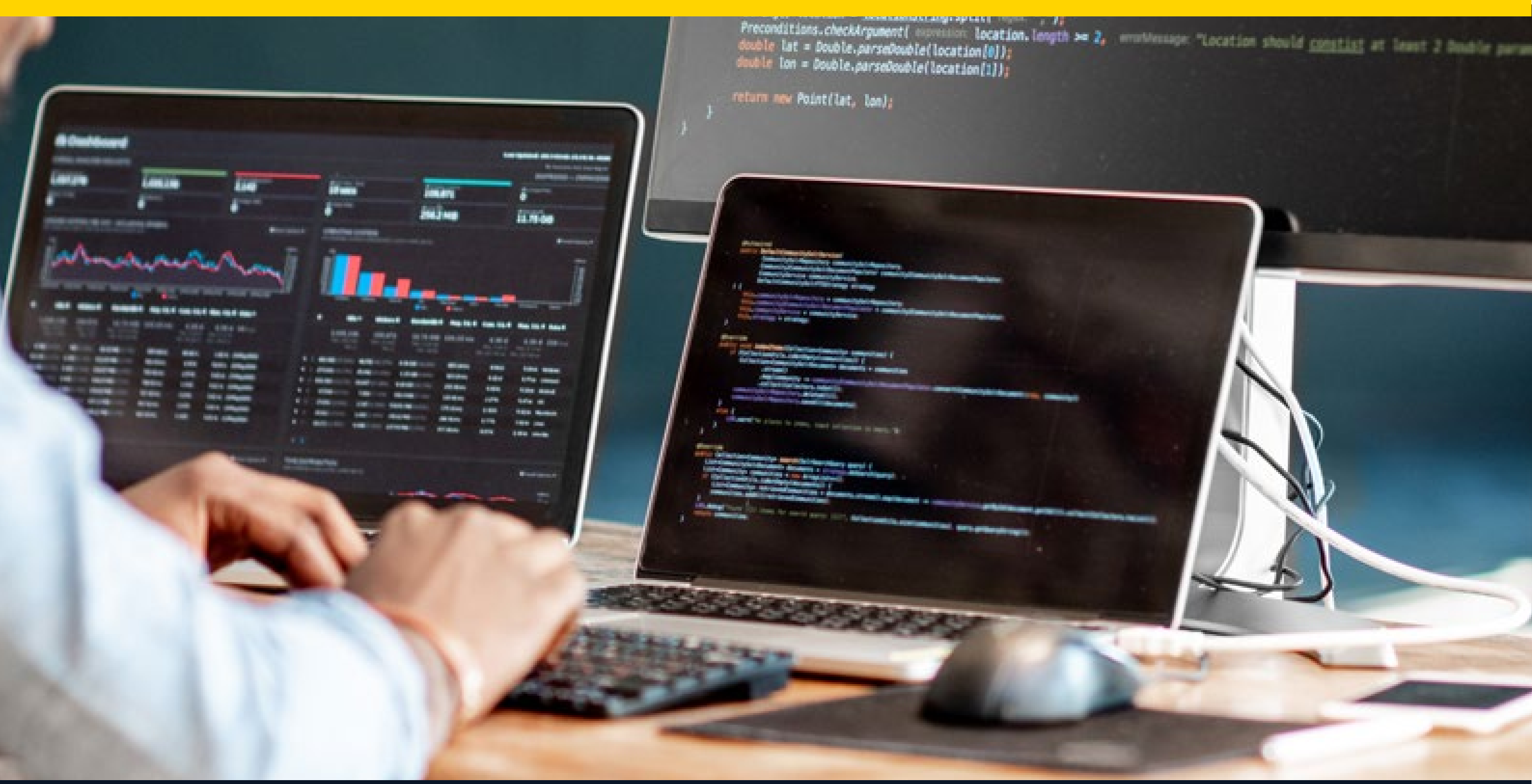
Gap assessment, development of an appropriate privacy framework and policy development should be carried out to as part of data breach management. Risk, compliance and legal teams need to work together with internal technology teams on identification of gaps or non-conformance, and any breaches as and when they take place.

Case study 4

A consumer products company designed and assessed their privacy and security posture for a new data driven marketing transformation project to help in incorporating security and privacy in their design. Data flows were documented for the security ecosystem to help understand the repositories that contained customer data by performing technical scans to identify HVAs containing customer PI and PIIs. Security and privacy controls and capabilities were assessed against NIST, GAAP and other standards to identify gaps and prepare detailed roadmaps for improvements.

The development of data ecosystem maps, interfaced with multiple stakeholders in marketing, security, privacy, etc. was done to develop a holistic view of the customer ecosystem to understand and map customer data locations. Technical scans and access control analysis were utilized to reduce the manual effort of providing keywords and iterative reviews. Auto-classification was performed based on PI-PII regular expressions and validated with stakeholders. With this, the company was able to assess their readiness for compliance regulations such as GDPR, CCPA and other regulations.

The digital transformation of corporate compliance



```
Preconditions.checkArgument( expression: location.length >= 2, errorMessage: "Location should consist at least 2 double para
double lat = Double.parseDouble(location[0]);
double lon = Double.parseDouble(location[1]);

return new Point(lat, lon);
}
```

29%

plan to invest over INR 10 crores to drive digital transformation over the next two years

The digitalization of compliance has picked up steam in the last couple of years. Organizations have been gradually leveraging technological tools and solutions for regulatory compliance and process improvements. The digital shift accelerated during the pandemic due to widespread disruption in operations, manage risks during remote working conditions and maintain business continuity. According to the survey, technologies such as FDA (35%), AI (37%) and real-time threat intelligence and endpoint security technologies (29%) are the driving digital transformation within compliance, risk and legal functions.

A strategic approach to investing in innovative technology and digital solutions to extract high value from risk and compliance programs will prove prudent in the long run. As per the survey, 29% stated their organizations plan to invest over INR 10 crores to drive digital transformation over the next two years, while 45% are looking at an investment between INR 1 – 10 crores.

Emerging technologies in a post COVID-19 world

AI, cyber forensics and RPA are the key technologies expected to be used regularly in compliance, risk and legal frameworks over the next two years.

Compliance in a post COVID-19 world will need an explosive recharge. As teams and budgets become leaner, risk, legal and compliance teams will need to harness emerging technologies such as AI, cyber forensics, RPA and blockchain to stay agile, resilient and effective. Revisiting technology infrastructure, machine learning and continuous monitoring would also play a pivotal role in driving the digital transformation of corporate compliance.

Uncertainties due to the pandemic have accelerated the need to use new technologies, including Regulation Technology, or RegTech in new ways. RegTech looks to transform the regulatory landscape by leveraging advanced technologies to enhance the compliance, risk and legal function. Companies should digitally transform from point-in-time compliance assessments to real-time (risk) management systems.

Limited involvement by the C-suite can be a challenge

31%

said C-suite involvement in the organization's digital transformation journey was limited to key matters only

46%

said that the CEO, MD or CFO was responsible to drive digital transformation within their organization. 11% cited the CIO and 34% said the CTO or Head of IT was responsible.

A successful digital transformation model needs to have high involvement of the C-suite, including the MD or CEO. As leaders, their role will be crucial in aligning digital priorities with their vision of the company, offering guidance to make it scalable and ensuring clear communication about the strategy and execution. However, the survey states that about a third of the C-suite are involved in only key matters. Jumping on to the technology bandwagon right now has become imperative to stay competitive and cost effective in the long run.

Forensics as a managed service - unlocking efficiencies through digitization and centralization

Adopting novel technologies, modernizing the existing technology environment, and digital training can improve the effectiveness, efficiency and impact of compliance programs. However, many companies still perceive this in as a cost burden and don't have a clear or long-term strategy outlined for implementation. Lack of requisite skillsets to optimize processes with the technology solutions is also a challenge.

32%

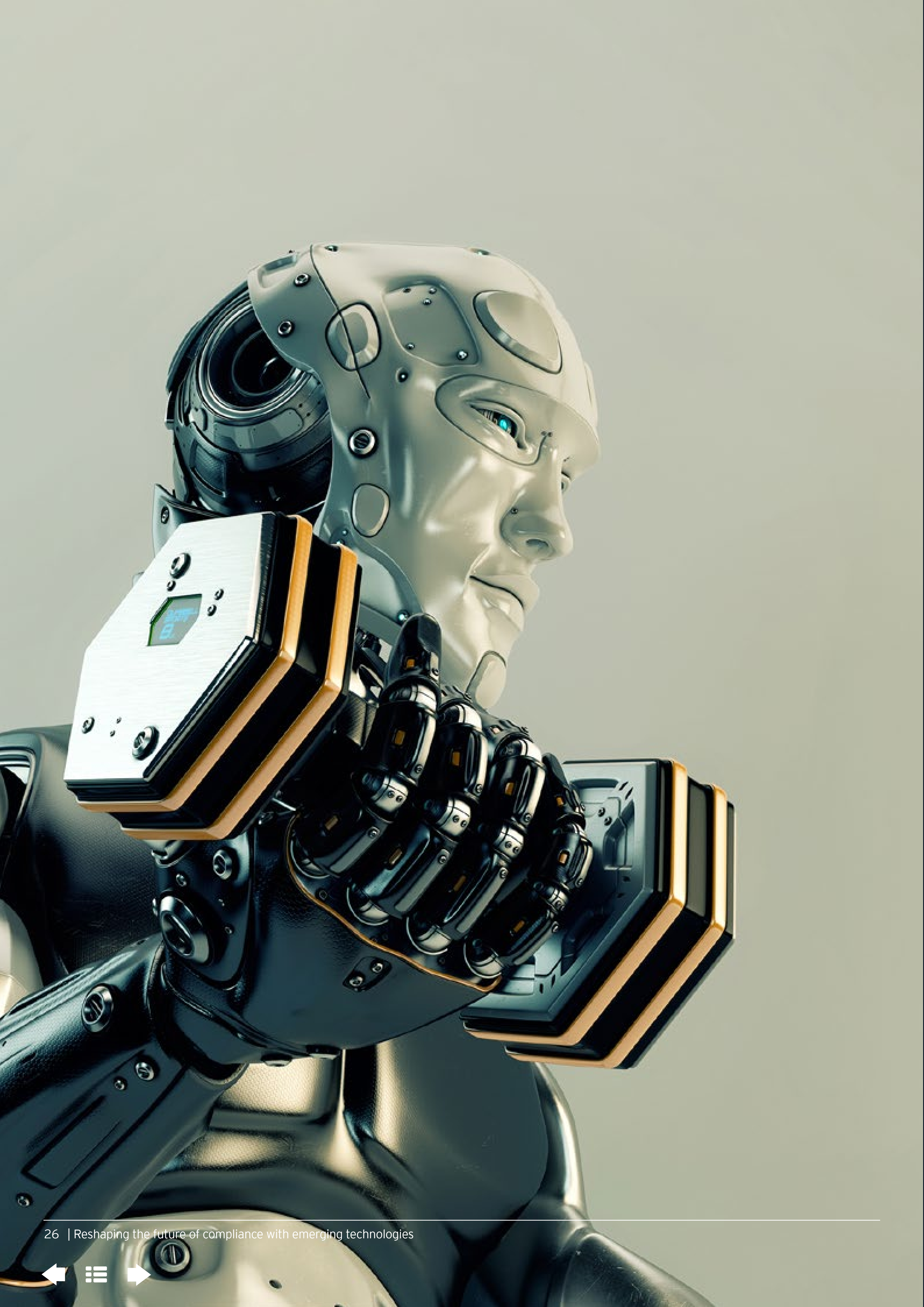
state high costs as a deterrent

25%

said that there was either a lack of clear strategy or a lack of expertise, knowledge and talent

Compliance functions may have fragmented use of technology as organizations are unable to leverage talent and technologies from one source.

Many global firms are exploring methods to centralize their compliance functions by creating a talent pool along with technologies to support their long-term business strategy. However, building and implementing a technology infrastructure can be expensive, thereby paving the way to outsource to third parties with an existing technology backbone and capabilities. Organizations can harness this model to transform and adapt new models of outsourcing the compliance and investigation functions.



In conclusion: reframing the future of compliance

Fraud, cyber and digital risks are set to rise even more in the new normal. Building compliance and risk frameworks, keeping technology at the heart of these programs in more important than ever before. A digitally empowered compliance and anti-fraud program that is well integrated across all business functions and guided led by the C-suite and board can maximize value, drive best practices within and augment adherence to fraud prevention policies and procedures. As leadership accountability increases, setting the right tone at the top forms a crucial element in laying the foundation for a robust anti-fraud and risk management program.

Companies that define, set and follow strategic imperatives are likely to have a better chance of weathering the storm. Some of these would be:

01

Investment in emerging technologies

RPA, AI, blockchain, cyber defense tools, data privacy and information governance technology – strung together as part of a GRC platform, or standalone, are all key weapons in the fight against fraud, and managing non-adherence to controls and overall better compliance management. The savings in the long run will far exceed the initial investments and bring substantial value.

02

Invest in the right processes and actions

Malicious actors and criminals are responsible for data breaches and attacks, followed by social engineering or impersonation-based incidents. These have augmented as a result of COVID-19 and the ensuing weak internal control environment. The right management team, the right technology and the right people – all need to come together to establish and lead a common goal to create, manage and update the right processes and remedial actions.

Leaders should strive to set the right tone, and invest in right technology, but all that will amount to very little, if compliance technology is not in the hands of trained personnel. Employees should also be given specialized training and reskilling opportunities (certifications etc.) to sharpen their skillsets.

Reskilling people

03

Management teams should set the right agenda and involve relevant stakeholders such as Chief Digital Officer, Chief Innovation Officer, Head of Compliance, Technology Head etc. They should work collaboratively and set the process of using technology to bolster internal controls and anti-fraud and compliance programs.

Set the right tone at the top

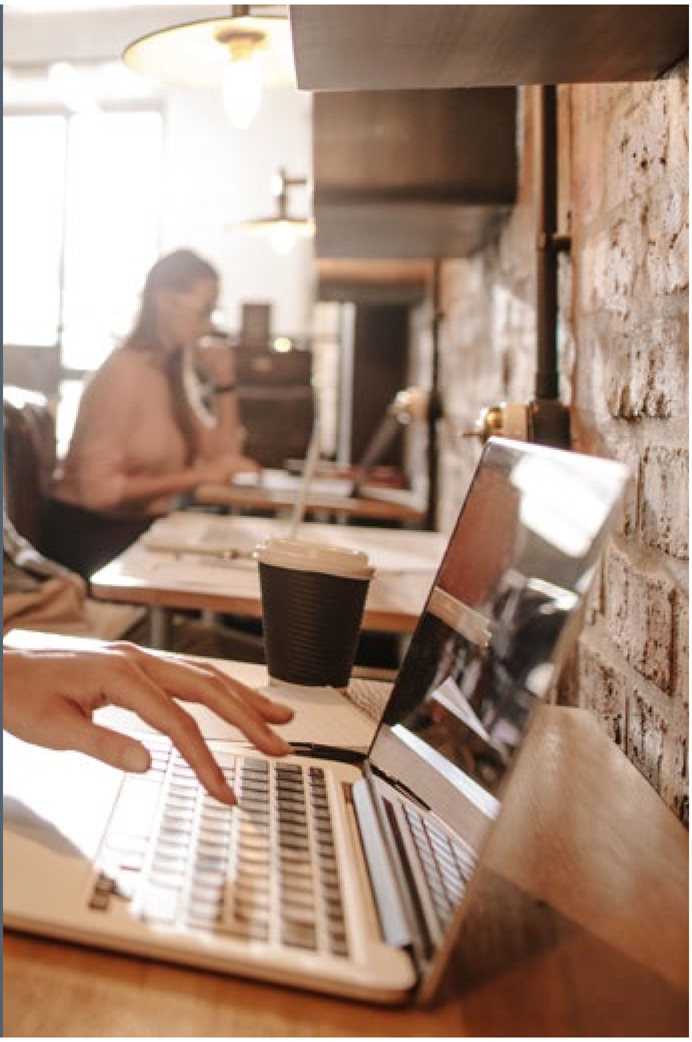
04

About the survey

This survey is jointly prepared by EY Forensic & Integrity Services in India and ACFE Mumbai Chapter. Its objective is to understand how technology is leveraged in risk, legal and compliance functions to mitigate fraud and other risks, emerging trends in cybercrime, data privacy and organizations' digital readiness in the new normal.

The survey was conducted through an online questionnaire and over 100 responses were received. The respondents comprised the C-suite and senior executives from functions such as finance, risk, legal, compliance, internal audit and technology, representing a mix of Indian enterprises as well as the Indian subsidiaries of multinational companies. They operated in a wide range of industries including banking and financial services, insurance, retail and consumer products, IT/ITeS, life sciences, manufacturing, automotive, oil and gas etc. All respondents are based in India. In addition to the survey results, the report includes EY's viewpoint based on the experience gathered in this field over a period of time.

Note: Some of the percentages in the charts total to more than 100%, since the respondents were allowed to make multiple selections.



About EY Forensic & Integrity Services

Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 4,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisors. We strive to bring you the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

About ACFE Mumbai Chapter

The ACFE Mumbai Chapter #160 was formed in 2011 and is a not-for-profit organization dedicated to fraud prevention education through meetings, seminars, workshops and professional networking opportunities for our members. Usually referred as ACFE Mumbai Chapter, it is registered as "Western Region Chapter of the Association of Certified Fraud Examiners (ACFE), India".

Our Vision is to create a community of fraud-fighting professionals in Western India.

Our Mission is to expand the membership through evangelization and outreach, create a platform for all fraud risk management professionals to share knowledge and support each other, provide thought leadership on prevention and deterrence of fraud and promote high standards of professional knowledge and ethics

Let’s talk

For help and more information, please contact one of EY Forensic & Integrity Services’ leaders.

Arpinder Singh
Global Markets and India Leader
Email: arpinder.singh@in.ey.com

Sandeep Baldava
Partner
Email: sandeep.baldava@in.ey.com

Vivek Aggarwal
Partner
Email: vivek.aggarwal@in.ey.com

Mukul Shrivastava
Partner
Email: mukul.shrivastava@in.ey.com

Anurag Kashyap
Partner
Email: anurag.kashyap@in.ey.com

Rajiv Joshi
Partner
Email: rajiv.joshi@in.ey.com

Yogen Vaidya
Partner
Email: yogen.vaidya@in.ey.com

Dinesh Moudgil
Partner
Email: dinesh.moudgil@in.ey.com

Jagdeep Singh
Partner
Email: jagdeep.singh@in.ey.com

Amit Rahane
Partner
Email: amit.rahane@in.ey.com

Vikram Babbar
Partner
Email: vikram.babbar@in.ey.com

Harshavardhan Godugula
Partner
Email: harshavardhan.g@in.ey.com

Vinay Garodiya
Partner
Email: vinay.garodiya@in.ey.com

Saguna Sodhi
Partner
Email: saguna.sodhi@in.ey.com

Prashant Behl
Partner
Email: prashant.behl@in.ey.com

Kulbir Kaur
Partner
Email: kulbir.kaur@in.ey.com

Ranjeeth Bellary
Associate Partner
Email: ranjeeth.bellary@in.ey.com

Shabarinath Kandala
Associate Partner
Email: shabarinath.kandala@in.ey.com

Kumar Polavarapu
Director
Email: kumar.polavarapu@in.ey.com

Uday Parmar
Director
Email: uday.parmar@in.ey.com

Avantika Ghildyal
Vice President – Marketing & Communications
Email: avantika.ghildyal@in.ey.com

Ernst & Young LLP

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EYG member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/en_in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

EYIN2107-004
ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

ey.com/en_in

@EY_India EY|LinkedIn EY India EY India careers ey_indiacareers