KPMG

CII
Confederation of Indian Industry

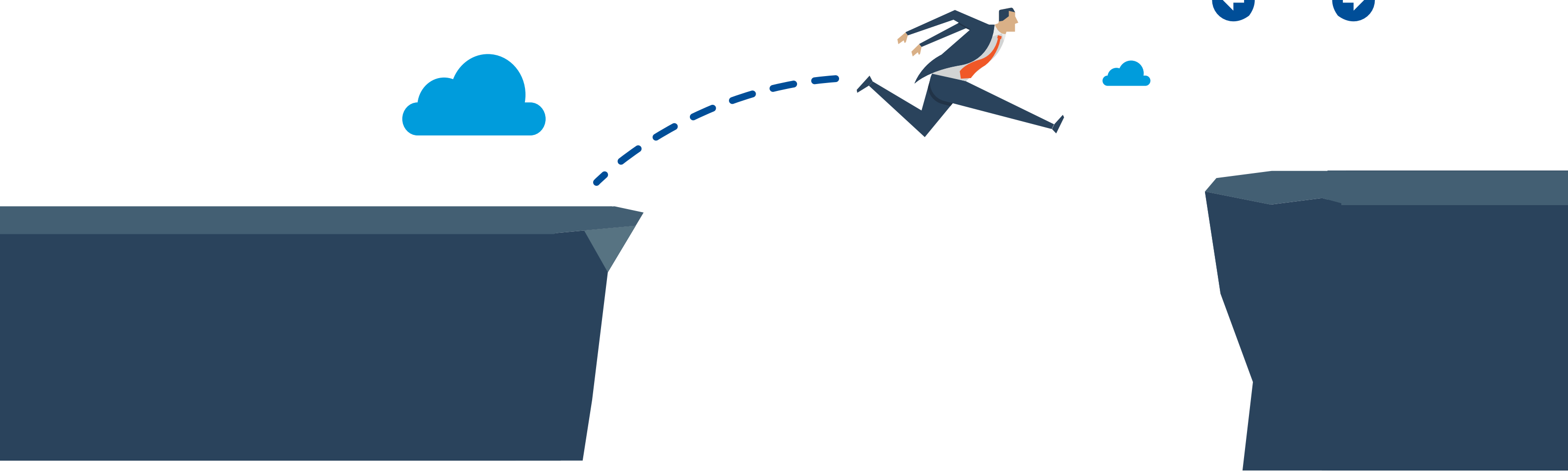
De-risking India in the new age of technology

Risk Consulting

August 2016

KPMG.com/in | cii.in

Table of contents



Executive summary

On his visit to India, Dr. Jim Yong Kim, President, World Bank stated that India is one bright spot in the global trend of sluggish growth. This comes at a time when the domestic market is upbeat about unprecedented opportunities in an emerging India. We are rapidly adopting and adapting to newer ways of doing business in a technologically challenging environment. The growth traction exposes us to a wide gamut of social, cultural, environmental, regulatory and geopolitical risks.

From drones to smart offices, new age technologies have not only transformed the traditional way of doing business but have also given way to unforeseen risks that can lead to serious consequences, if they go unmanaged. It is imperative to understand the ramifications of such transformational technologies and design appropriate risk management strategies to de-risk our environment.

KPMG International recently conducted a Global CEO Outlook Survey 2016, wherein it was found that 91 per cent of the CEOs are concerned about the impact of global economic factors, 92 per cent of CEOs are concerned that regulations will inhibit their growth and 77 per cent acknowledged that cyber risk management is now a key responsibility matter.

India is significantly dependent on international markets for driving domestic growth. This makes businesses vulnerable to global geopolitical developments, a fact clearly reflected in the CEO survey. Indian financial services businesses are integrated with the global financial markets more than ever before, and this significantly impacts overseas transactions that Indian businesses enter into. Any significant business decision must also be looked at from a cybersecurity perspective. A Merger and Acquisition (M&A) deal for example, must deal with data breaches or probable regulatory violations before it is executed. People across all levels need to be aware of cyber issues and its impact on the performance of the organisation. With advanced smart systems and robotics being introduced to improve efficiencies, it gives rise to the risk of managing human capital. Strong corporate governance will play a significant role in managing such risks and enhancing the overall organisational brand and reputation.

Another area of challenge is developing technology-enabled risk analytics that adequately protect the organisation from frauds and manage crisis before it hits an organisations' operations. The identification, assessment and prioritisation of risks followed by procedures to monitor, minimise and control their impact is the very essence of risk management.

The recent cyberattacks on certain government bodies is an illustration of inadequate risk management. Cyberattacks like these pose a serious threat to economic growth and must be tackled using more advanced risk management technologies. Data breaches and cyberattacks are a common affair. Ignoring these risks can lead to potential liabilities, substantial revenue loss and a damage to reputation.

The complexity of technological developments coupled with the unpredictability of their evolution makes the process of managing risks more critical and harder for individuals as well as regulatory bodies. Hence, risk management must top the agenda of every board and keep pace with the dynamic regulatory landscape of India and emerging technologies to safeguard themselves against the consequent undesirable outcomes.

Exploring the challenges that organisations face and then following better risk management practices is the first step to de-risk India in the accelerated environment of cognitive technologies,that can unlock the true potential of organisations by balancing the risks and opportunities.

Mritunjay Kapur

Partner and Head

Risk Consulting

KPMG in India

Foreword

Over the past year, there has been a strong positive sentiment among India Inc. on account of several factors affecting the domestic market. At the same time, the global turmoil is showing no respite. Today, India Inc. is among the top drivers of growth globally. However, the business dynamics are changing more rapidly than ever, riding high on technological changes.

The government on its part has been fairly successful in projecting an image of a reformist regime. Several regulations are lined up and some critical reforms in taxation are well on their way to become laws. Once implemented they promise to bring in more transparency and potential benefits to the nation. How organisations embrace such changes in regulation is what is key.

The changing business, regulatory and technological environment invariably brings with it a gamut of new risks, which compel organisations to adopt different risk management strategies. Volatile geopolitical environments, Brexit and potential leadership changes in certain large global economies are likely to have a significant impact on Indian businesses. The intensification in the integration of India Inc. with other global economic powerhouses, is only a matter of time. With this integration, the impact of challenges can bolster further.

In this publication, we attempt to analyse the potential of risk management strategies as an effective tool for riding the growth wave for Indian industries using technology in its favour and be a part of a larger success story.

The report analyses management strategies in various areas including financial services, globalisation, multiple taxation risks, future risks in smart technologies and robotics, cybersecurity risks, crisis management, risks in acquisitions and joint ventures, regulatory risks and human capital risks amongst others.

An in-depth study of these critical areas can help organisations develop a perspective on effective risk management, mitigating risks, analysing risks and consequently, devise the way forward.

We hope you find this publication useful. As always, we look forward to your feedback on the same.

Mritunjay Kapur

Partner and Head
Risk Consulting
KPMG in india

The early 2000s saw the beginning of Information Technology boom in India and made it the preferred IT destination in the world. With availability of talent and increased telecom bandwidth, Indian companies could deliver world class solutions to global customers.

A recent phenomenon is the digital age dawning and growing at a rapid pace. There is a new culture of startups and the introduction of new age technologies such as Internet of Things (IoT), machine learning, big data analytics, artificial intelligence, computer vision, augmented and virtual reality and internet security. It's about building the enterprise software platforms, not merely implementing them and also innovating and improving on them.

The accelerated growth of the digitalization and technology also poses a significant challenge to many companies' business models as well the inherent risks involved. Risk management is an imperative for an organisation because without it, a firm cannot possibly define its objectives for the future. If a company defines objectives without taking the risks into consideration, chances are that they will lose direction once any of these risks hit home.

This conference aims at shedding light on the various risks accompanying the influx of new technology that is currently seeing a tremendous growth in the sub-continent. Further topics that would also be discussed will encompass the need of an effective risk management in place, mitigating risks, analyzing risks and the way forward. On behalf of CII and KPMG we would like to thank the sponsors, industry experts who have graciously contributed their time and energy into this endeavor.

Suresh Senapati

Chairman
CII National Risk Summit 2016
Former Executive Director & CFO
Wipro Ltd

Strong corporate governance to enhance the organisational brand and manage reputational risk

Purushothaman K G

Partner

Governance Risk and
Compliance Services
KPMG in india

Deepak Viegas

Director

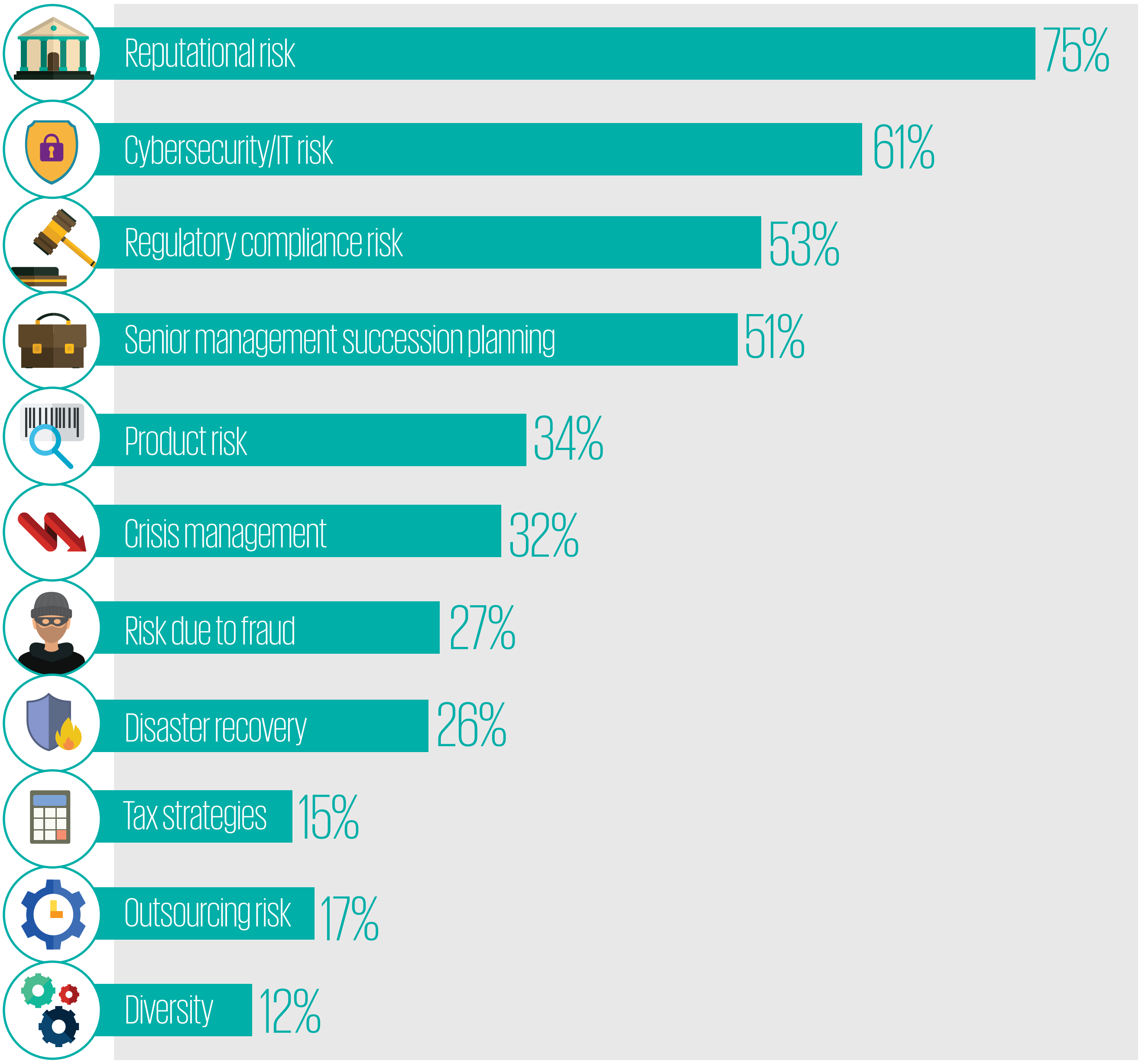
Governance Risk and
Compliance Services
KPMG in india

> It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.[01]
>
> Warren Buffet

Warren Buffet's statement resonates well with the turn of events in the recent years. There have been many well-established organisations and individuals who have faced defining moments that, depending on the choices they made, determined their survival beyond the key turning point. It is how organisations prepare for and handle these moments that define their future reputations and brand value. Due to the enhanced use of social media and technology, information is available to large audiences very quickly. Negative information may go viral and affect the company image.

According to Eisner Amper's 6th Annual Board of Director's Survey published on 20 January 2016, 'Reputation remains a leading concern; cybersecurity a growing threat.'

Risk confronting boards



[01] "The three essential Warren Buffet Quotes to live by" dated 20 April 2014 by James Berman.

Organisations strive to put in place good corporate governance practices and leadership to protect their brand image in the light of major instances of corporate misdeeds. Good corporate governance is recognised as a crucial element for upholding and sustaining investment climate for aspiring companies and well organised financial markets.

Sir Adrian Cadbury, in his report dated 1 December 1992 under The Committee on the Financial Aspects of Corporate Governance says that "Corporate governance is the system by which companies are directed and controlled."

The OECD Principles of Corporate Governance state: "Corporate governance involves a set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined."[02] The OECD principles as a reference point for good corporate governance, presentation by Grant Kirkpatrick corporate affairs division, OECD.

When implemented effectively, corporate governance can avert corporate misconducts, frauds and the liability to the company. It also magnifies the company's image in the eyes of the public as a self-policing company that is responsible and worthy of their investment and trust. It represents the ideology, practice and culture of an organisation and its employees. Corporate governance keeps a company candid and free from troubles. If this ideology breaks down, then the company may face trouble, distrust and disgust of stakeholders. On the other hand, good corporate governance mechanisms seek to protect an investor's confidence and maximise corporate value as well as increases the worth of company in capital markets.

The SEBI Listing Obligations, 2015 and the Companies Act, 2013 have introduced some progressive and transparent processes which benefit the stakeholders, directors as well as the management of companies. The processes have not only raised the bar of corporate governance but have also aligned them more closely with international leading practices.

Key building blocks of sound corporate governance

- Board structure, roles and duties
- Board committees
- Risk management
- Internal Financial Controls (IFCs)
- Internal audit
- Ethics framework
- Compliance framework
- Disclosure and reporting

[01] The OECD principles as a reference point for good corporate governance, presentation by Grant Kirkpatrick corporate affairs division, OECD.

Board structure, roles and duties

The actions of Boards are scrutinised minutely by the stakeholders, regulators, politicians, media, etc. Composition of the board and leadership are vital in supporting a Board's ability to discharge their duties effectively. Boards need the right mix of skills and experience and should be aware of the fact that the 'right' mix changes over time. They also need a leader who will ensure that the Board discharges their duties effectively and a process that engages them in a prolific manner. Achieving efficacy is indispensable for Indian boards today, with an increased focus on independence.

Companies should make an investment in high performance governance structures by putting resources into:

- Director appointment and evaluation
- Board succession planning
- Infrastructure
- Board education and ongoing development
- Governance process tools, including but not limited to Director role descriptions, policies, committee charters, dashboards, succession planning templates, self–assessment instruments and techniques for making board meetings effective.

Board committees

Committees can work best with the right people in the right roles. One of the biggest challenges for them is to identify suitable members amongst the available skill-set.

Companies should:

- Identify the right mix of skills and expertise amongst the existing directors to best fit the role
- Define the terms of reference for each committee
- Conduct an annual evaluation of the committee
- Define the agendas and reporting mechanisms for each of the committees.

Risk management

It's now invariably acknowledged that, given the complexity of business and other factors, risk can emerge instantly and unpredictably from anywhere, causing increased uncertainty and volatility. This uncertainty increases the need for precise data and the need to ensure that the decisions take into consideration various alternatives and options. It is vital to find the right balance between risk aversion and risk taking. This requires companies to thoroughly understand the complexities associated with the company's activities. Implementation of Enterprise Risk Management (ERM) is rarely found easy by a company. It requires a rare combination of organisational commitment, strong executive management and the willingness to understand the sensitivities of the programme. Regardless of the effort required, ERM is worth it because it drives organisations to identify and evaluate their risks, which is the first step towards enhancing shareholder value and protecting capital.

Companies should:

- Choose a governance structure that fits the company
- Develop an ERM framework and embed it in the business rhythm
- Create a robust intelligence system by leveraging technology
- Discuss emerging risks such as cybersecurity and update the risk registers every quarter and should build mitigation plans
- Formally designate an individual to serve as the Chief Risk officer (CRO) or Head – Risk Management Executive
- Present risks quarterly to the risk management/audit committee. The top 100 listed companies are required to constitute a risk management committee as per the Listing Obligations, 2015
- Define an oversight structure which should clearly state the responsibility and accountability of designing, implementing and monitoring risk
- Develop strong ERM policies and procedures including an effective anti-fraud programme
- Establish reporting processes to ensure that the board of directors are getting the desired information for understanding and assessing risks
- Maintain an effective communication mechanism amongst the stakeholders, customers, boards of directors and employees.

Internal Financial Controls (IFCs)

Section 134 of The Companies Act, 2013 defines IFC as, "The policies and procedures adopted by the company for ensuring the orderly and efficient conduct of its business, including adherence to the company's policies, the safeguarding of its assets, the prevention and detection of frauds and errors, the accuracy and completeness of the accounting records and the timely preparation of reliable financial information."

Companies should:

Particulars	Utilities
Assess the governance tone at the top	• Define entity level governance policies like a whistle blower, code of conduct etc. • Define process level policies and procedures • Develop delegation of authority.
Identify key and non-key controls	Perform an assessment of: • Entity level controls • Process level controls • IT controls • Fraud controls.
Document all the existing financial and operating controls	• Develop a robust financial process and document controls around the process • Document controls in the form of Risk Control Matrices (RCMs) • Controls on accuracy of judgement and estimates • Define and document user responsibilities.
Monitor effectiveness of the existing controls	• Consider implementing an ongoing framework for monitoring and evaluation of the defined controls and internal certifications • Perform periodic assessments to review the operating effectiveness of controls
Consider preventive and detective anti-fraud controls	• Carry out a fraud risk assessment and identify the fraud risks and existing controls in the processes • Define the mitigating controls for any gaps identified.
Review technology support	• Review the existing technology structure and the use of information technology modules/ software • Ensure adequacy of information technology general controls and information technology application controls • Consider automation of routine activities to reduce incidence of manual errors.
Develop an extended control landscape	• Financial reporting controls • Fraud implications • Controls to address financial assertions • Operational controls • Efficiency/service implications • Quality/technical control.

Internal audit

The role of an effective Internal Audit (IA) function today is much more than simply compliance. With increasing market volatility and complexity, internal audit is expected to deep dive and add in value beyond assurance, particularly in the areas of strategy execution and risk management with an increased usage of analytics and technology.

Companies should:

- Ensure that governance, risk and compliance is an inherent part of the risk management process
- Move towards a continuous internal audit approach
- Co-source/outsource or develop an in-house internal audit function
- Formulate an internal audit manual detailing the scope, functioning, and periodicity, the reporting framework and the methodology for internal auditors
- Strategies the communication mechanism between internal audit, management and the audit committee
- Conduct a separate meeting of the internal audit team with the audit committee, once a year without the presence of the management.

Ethics framework

Governments and regulators globally are enforcing laws more rigorously, and are passing new laws and regulations actively. Universally it has been realised that the challenges businesses face are not just related to market products, but rather lies in making the process socially acceptable. The problem multiplies when employees live in a culture where their values and norms that may conflict with the rules or conduct that the company desires to enforce. Any misconduct can propagate negative publicity for the company and bring a major reputational loss to the company.

Companies should align and balance the interest of the company, employees and stakeholders:

- Establish practices, behaviours and ethical values throughout the company
- Set a communication mechanism between the management and the employees, which illustrates leading ethical standards and puts in place adequate barriers which eradicates ethical malpractice
- Lay down a code of conduct
- Devise a whistle blower policy and arrange hotline numbers and e-mail addresses to report concerns. Create an environment where employees feel comfortable to open up and raise their concerns without any fear and hesitation
- Implement an internal audit mechanism to monitor the ethical issues faced as well as the actions taken to resolve them.

Compliance framework

Complexities and an expanding horizon of regulations have made it challenging for all organisations including sophisticated business to meet the increasing ethics and compliance demands. The risks faced by organisations are changing drastically and very frequently. The key issues these organisations face in addressing the growing regulatory challenges are, first, the quantum of regulatory change; second, organisational structures and commitment; and third, the role of the compliance function. Apart from these, companies face unprecedented scrutiny from regulators around the world, who are approaching enforcement with great robustness and new technological tools. Activist shareholders, employees, customers, NGOs and other stakeholders also put companies under the magnifying lens, and social media validates and empowers perceptions.

Companies should:

- Develop an effective compliance strategy
- Develop a comprehensive framework of laws and regulations
- Develop a compliance checklist to ensure compliance and obtain management/process owner sign-offs
- Review and monitor the compliance status on a periodic basis
- Develop an online software tool to manage compliance requirements of the company which can populate Management Information System (MIS) on a periodic basis and generate auto alerts for meeting timelines.

Disclosure and reporting

- Companies face numerous challenges from various stakeholders, the government, consumers, etc. in order to provide precise and reliable information swiftly and more efficiently. The quantum of disclosures has increased and regulators and standard setters are now more closely scrutinising the effectiveness of disclosures made. The cost pressures are also building up with enhanced disclosures and reporting requirements; and hence companies have to strive to report and disclose faster and more effectively with fewer resources.

Companies should:

- Develop, review and update a comprehensive checklist detailing all the disclosure requirements
- Simplify and standardise processes, effectively leveraging technology for real–time status tracking.

Conclusion

'Good corporate governance' is simply 'good business'.[03] The primary purpose of corporate governance is to enhance the shareholders' value and protect the interests of other stakeholders by improving corporate performance and accountability. Hence, it assists the company to strike a balance at all times between the need to multiply shareholders' wealth while not in any way being inimical to the interests of other stakeholders in the company.

Further, it promotes an environment of trust and confidence among those having competing and diverging interests and thus helps build a sustainable brand and reputation.

> The way to gain good reputation is to endeavour to be what you desire to appear.
>
> Socrates

[03] http://www.archive.india.gov.in/business/corporate_governance/concept_objectivess.php accessed as on 4 August 2016

Cybersecurity - redefining how to protect the business

Ninad Purohit

Technical Director
IT Advisory Services
KPMG in india

Cybersecurity - A paradigm shift

Cybersecurity

While organisations have traditionally focussed on ICT security, fringe areas which do not directly fall under the domain of traditional ICT, have usually been neglected. Such areas include, but are not limited to, Building Management Systems, Physical Access Control and Surveillance systems, SCADA and Engineering Control Systems, Telecommunications Equipment and personal communications equipment used by staff, etc. and can be clubbed into the domain of 'cybersecurity.'

While ERP, payment and other systems that directly affect financial reporting have enjoyed security focus, other systems which generally get classified as 'non-critical' largely remain insecure.

As more and more of these systems start getting connected to each other and to the internet, we see a paradigm shift in terms of 'What's critical?' Internet of Things (IOT), Bring Your Own Device (BYOD) and increasing level of outsourcing and sub-sourcing complicate things further. Cars that drive by themselves, robotic surgery that happens through remotely connected doctors, control systems that mix molecules to produce medicine and systems which control nuclear centrifuges are just some of the examples of 'at –risk' systems.

Personal communications and computing devices used for official work exacerbate this risk further. A wearable device used to track fitness, connected to a mobile phone used to receive a text message or e-mail and mobile applications with access to each other's data could be used to steal critical information. These mobile devices which are usually unmanaged, as they get connected to the organisation's wireless LAN can also potentially introduce malware into the environment.

We see the cyberattacks becoming more and more targeted. Many of the cyberattacks in the past few years used spear-phishing and targeted social engineering as a vehicle to launch targeted malware.

While traditionally cyberattacks were largely used for causing financial and reputational loss, today they have a potential of posing a threat to human life. While the perpetrators behind these attacks traditionally were a few challenge loving 'hackers' with unbridled curiosity, we see an increasing number of state sponsored cyber terrorists and organised criminals behind the attacks today.

> Luckily, while the areas and methods of cyber-attacks have changed and advanced, the basic preventative hygiene principles still hold good. While attacks and technical controls race with each other as they always will, a majority of the attacks could be averted with some basic security hygiene.

It begins at the top

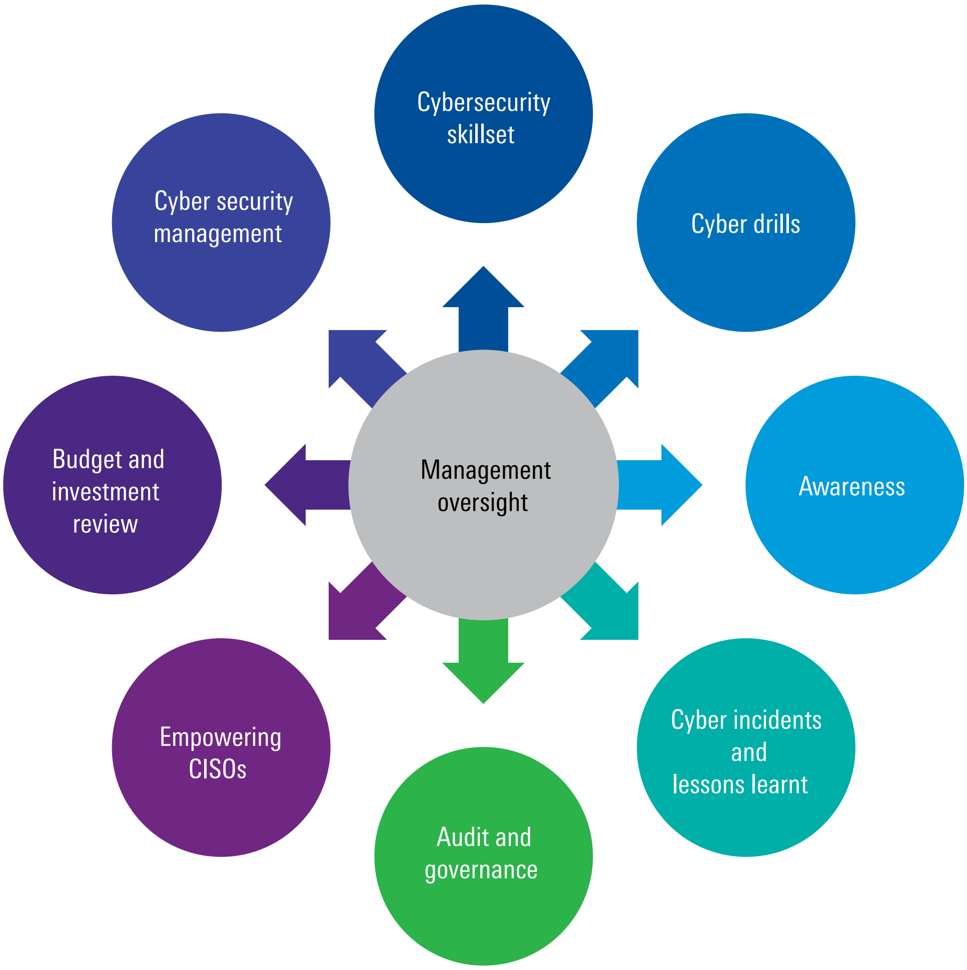
Cybersecurity – A Boardroom discussion

Cybersecurity unlike IT security is not limited to IT systems. It spills over into the areas such as but not limited to, human resources, administration, telecommunications, instrumentation, etc. and hence requires the involvement of the senior management to provide the requisite amount of governance and oversight.

Cybersecurity has started gaining visibility at the top level and is now an essential part of the Boardroom discussion. Regulators are increasingly making the Board members and senior executives of the company accountable for cybersecurity for their company, often with stiff penalties including but not limited to heavy fines and legal consequences. The senior management and the Board therefore needs to be aware of the cyber threats to their organisation and cyber-incidents happening both externally and within their organisations

The senior management also needs to review the effectiveness of the investments it makes towards security controls. While security investments do not have a tangible ROI, the review should include an assessment of cyber risks, cyber incidents and lessons learnt from these incidents. Auditors, both external and internal can play a crucial role here. While the general tendency so far has been to do the bare minimum required to comply with regulations or to achieve a certification, the actual adequacy of the organisation's cybersecurity programme should be evaluated.

The Board and senior executives should also take a stock of adequacy of the cybersecurity skillsets within the organisation. These need to be strengthened via requisite training and hiring. The Board needs to empower the CISOs/Cybersecurity officers to take required decisions to protect his/her organisation.



While the adage 'penny wise pound foolish' holds true, an organisation cannot spend a million to save a few hundred. An estimate if not the actual impact of a cyber-incident should be evaluated vis-à-vis the investments required. It may at times be necessary to accept certain tolerable risks. At other times, a 'cyber insurance' may seem appropriate.

> Lastly but most importantly the senior management needs to lead by example. Nothing can undermine an organization's Security policies and controls more than failure by its senior management to abide by them.

Preventive medicine

Basic hygiene

Cybersecurity has its own challenges. Several of them however, can be addressed with some basic hygiene.

Basic steps such as changing the default usernames and passwords for computing equipments, stopping unnecessary services, modules and ports on servers controlling physical access to critical infrastructure, a robust patch management regime and an antivirus program go a long way towards averting a cyber-incident. It's important however to look beyond the standard ICT environment to assess other equipment which may require security hardening.

Human resources and third party de-risking

Insider threats, corporate espionage, cyber-frauds and terrorism threats make employee and contractor background checks imperative. Most organisations do not verify their staff's antecedents beyond their employment and academic history. Criminal history checks, especially for staff involved in handling critical infrastructure and applications may help avert certain cyber incidents. A robust separation process also helps maintain adequate access controls.

With the increasing trend to outsource various activities, organisations need to ensure that their data continues to enjoy the same level of protection as it would in their own control. Remote access to critical infrastructure also needs to be controlled. Auditing vendor premises periodically helps reduce the risk of outsourcing. A road-block that many organisations face is the absence of 'right to audit' clause in their vendor agreements. The deficiencies discovered during such audits should be tracked to closure.

Cybersecurity – Adopting an onion ring approach

Reliance on a single control such as a firewall and SSL certificates often leads to organiasations getting complacent about their organisation's security.

Security controls should always be multi layered. While controls such as firewalls, intrusion prevention systems, anti-distributed denial of service systems, web application firewalls and Anti-Advanced Persistent Threat (APT), take care of perimeter security, an organisation is often at risk from entry points such as unsecured wireless access, open LAN ports in visitor areas, and remote access mechanisms.

While encryption is used for confidentiality, authentication, integrity and non repudiation requirements, insecure implementations and deprecated versions of SSL and weak encryption algorithms defy the very purpose of such systems.

While infrastructure components get the necessary security care, applications are often neglected. Insecure coding and design are responsible for several cyberattacks. Many organisations today do not follow the traditional Software Development Life Cycle (SDLC) methodologies and are shifting more and more towards agile development. Dev-Ops and Shadow-IT exacerbate this risk further.

Of about 3000 types of known attack methodologies, 900+ are related to exploitation of software and hardware vulnerabilities. Ensuring security throughout SDLC and effective vulnerability management programme goes a long way towards securing these components.

The weakest link

A chain is only as strong as its weakest link

An organisation may implement all the required technology controls but may still fail to prevent or detect a cyberattack if the people operating these controls don't operate them correctly or consistently. Security in business processes and security procedures therefore becomes crucial.

People themselves need to be aware of these controls and the policies and processes of the organisation. Quite often they are not aware and thereby become the weakest link. As technology controls become stronger and difficult to exploit, cyber-attack perpetrators often take the aid of social engineering techniques to bypass these controls. Social engineering exploits human emotions such as fear, greed, sympathy and the general tendency to help others.

Today's cyber-attacks are often multi-staged. While the attack finale may be very dramatic and may use an Advanced Persistent Threat (APT) or a specially crafted malware, it usually begins with a simple social engineering attack.

While we now have general awareness about phishing and Nigerian princes, the phishing attempts have become more and more targeted (spear phishing) and difficult to identify. The phishing attempts today are not restricted to e-mails, they also take the form of fake recruitment websites, fake websites that mirror actual websites, social media identity impersonation and similarly spelt web addresses and nicknames and even direct phone calls.

Organisations need to ensure that their employees and contractors are aware of such traps and that they know how to handle and report them. As the attacks get more and more innovative, organisations need to play the catch up game and refresh their staff's awareness. These awareness trainings need to be at all levels. There is an increasing tendency of social engineering targeted at senior executives, and secretarial staff.

> An organisation may test the cybersecurity awareness of its staff through tests, quizzes, games and mock incident drills to assess the adequacy of its awareness program and to identify improvement areas.

And yet...

Preparing for the worst

Cybercriminals and cyber-defense professionals are always in a race to outdo each other and sometimes it may so happen that the criminals win.

An organisation can make every effort to prevent a cyberattack. It may have the best possible technology and process controls. An attack may still be successful.

In such an event it always helps to be prepared. Many organisations concentrate only on the preventive and detective controls and fail to strengthen their reactive controls. Many business continuity and disaster recovery plans do not consider cybersecurity risks or their resilience plans

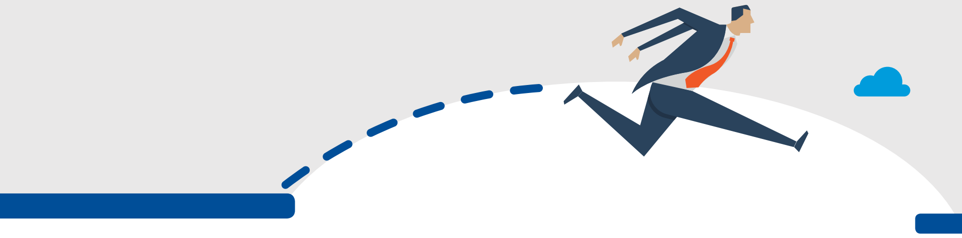
Organisations need to evaluate if their staff is adequately equipped to detect, defend, contain and respond to a cyber-incident. While organisations invest in SIEM and other monitoring mechanisms, they fail to invest in building their incident management skills. Quite often the Security Operations Center (SOC) staff does not know whom to contact if there is a cyber ncident. A cyber escalation matrix, if it exists is often not updated. Much time is therefore lost in responding to a cyberincident.

Board members and senior executives are often unaware of cyber incidents occurring in their organisations.

Organisations should periodically evaluate their cyber incident response capabilities. This can happen either via mock cyber war drills or through table top paper simulation exercises. Senior executives and board members can act as observers in such drills.

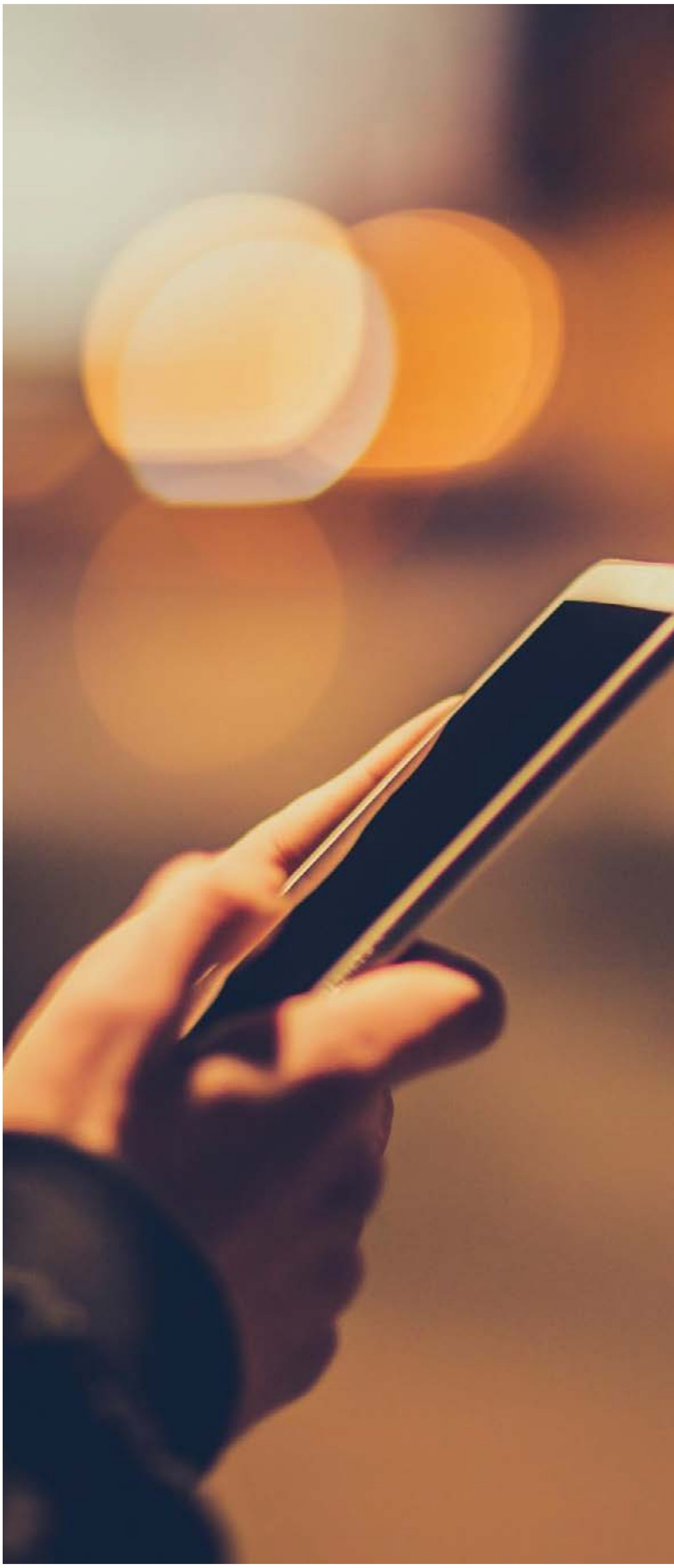
A cyber Incident can potentially cause an adverse impact to an organisation's brand, reputation and the trust of its customers and shareholders and hence, information flowing out of the organisation during such an incident needs to be controlled.

It is recommended to keep an approved press release message and to nominate a designated spokesperson to manage and control communication with the outside world during a cyber incident.



Summary

- Cybersecurity is no longer restricted to standard ICT domains and encompasses multiple areas of an organisation including but not limited to human resurces, supply chain management, sdminstration and infrastructure and therefore requires governance at the highest levels.
- Board members and senior executives of organisations are increasingly being held accountable for cybersecuriy incidents in their organisations and hence need increased visibility in to the organisation's cybersecurity posture and cyber incidents occurring both within and outside their organisations and need to assess if their organisations are equiped with the right tools, processes and skills to address such incidents adequately.
- Board members need to provide sufficient commitment and support to the organisation's cybersecurity staff. This support required may be in terms of devoting sufficient time, budgets and resources or empowering the security personnel with the right delegation of authority.
- An organisation can't rely solely on technical controls to avert a cyber incident. It needs a combination of the right people, processess and technology to prevent a cyber Incident.
- Lastly, organisations need to be prepared to adequately deal with a cyber incident and should be capable of responding and recovering from such an incident.



Human capital risks

Introduction

The term 'human capital' refers to the stock of knowledge, habits, social and personality attributes, including creativity, embodied in the ability to perform labour so as to produce economic value[01]. It is one of the organisation's intangible assets that are not directly reflected in the financial statements, but are very critical to the overall health of a company. In terms of the popular brand equity logic, employee-based brand equity drives customer-based brand equity, which in turn, drives the financial-based brand equity of the firm[02]. However, given the fact that human capital as an asset to the firm can be very transient in nature, executives cannot undermine the importance of managing the risks associated with them.

Human capital risks are employee-related events or behaviours that can negatively affect the operations and/or value of the company. These risks may be generated by activities either inside or outside the workplace[03].

[01] Becker, G. S., Human Capital, University of Chicago Press Economics Books, 1994.

[02] King, C., & Grace, D., Building and measuring employee-based brand equity, European Journal of Marketing, 2010.

[03] Selene, I., Human capital risks associated with change, AON conference presentation, 2008.

Vishalli Dongrie

Partner

People and Change Advisory
KPMG in india

Types of human capital risks

Human capital risks can be primarily of two types:

1. First order risks: These are basic level risks that have a direct cost implication to the firm and can be managed using relatively objective approaches. For example, risks associated with talent attraction, attrition, fraud and compliance.
2. Second order risks: These are complex risks that have a detrimental impact on the firm in the long-term and require strategic approaches for management. For example- risks associated with brand image (brand sabotage by employees), capability and capacity.

Both the types of risks are critical and need to be managed with significance for a firm to remain healthy. However, first order risks are encountered with high frequency and thus, need stringent ongoing monitoring and management mechanisms. Second order risks are influenced by the first order risks and do not show their impact instantly. They need to be managed with deeper level interventions, driven by the top management.

First order risks

Talent attraction risks

Employer's brand image in the market and Employee Value Proposition (EVP) of the firm are crucial factors for attracting the right talent. Given the scarcity of talent and the growing interest of organisations in evaluating the person-organisation fit before hiring, it is important that the employer brand appeals to the target segment in a specific way. Firms are increasingly investing in promotions of the employer brand through formal channels, such as best employer surveys. However, low differentiation in employee value proposition, high competition for the limited pool of talent and rising popularity of employee review forums that are considered more reliable than other paid promotion channels[04, 05], are factors that pose risks to the talent attraction efforts of a firm.

Developing and communicating targeted and distinctive employee value propositions, paying attention to informal employer branding channels alongside the formal channels, strengthening social media image management capabilities and appropriately positioning the employer brand are some of the risk mitigation strategies companies can adopt.

Attrition risks

Attrition is a costly phenomenon for a firm with both direct and indirect cost implications. Separation costs, temporary staffing, replacement costs and training costs are some other factors that have direct cost implications on the firm. Lost productivity, learning curve of new employees, lost knowledge, reduced morale and lost clients/opportunities are some of the factors that have indirect implications on the cost.

Risk management strategies can be built around pre-employment screening, interventions relating to the work environment (managers, peers, culture), employee engagement, development and growth opportunities and compensation and benefits philosophy (pay for performance, benchmarking, pay parity/bands).

Fraud risks

Corruption, internal frauds, cybercrime, asset misappropriation, intellectual property and financial statement frauds are common frauds that can damage the brand, an employee morale, company's share value, business-regulator relationships and have immense management costs associated with it.

Firms need to focus on pre-employment screening; defining and communicating the code of conduct; putting in place internal controls, fraud control strategy; strengthening internal audit; increasing focus on fraud awareness training, fraud detection strategies, and most importantly fraud reporting mechanisms (whistle blowing).

Compliance risks

Processes are established to strengthen governance mechanisms, comply with regulatory requirements and optimise operations. However, there is always a possibility of incompliance by a set of employees, which may weaken the governance mechanism, lead to faults on the regulatory front, and have cost implications due to suboptimal operations.

Risk management strategies should be built around monitoring process compliance, establishing and creating clear guidelines, training and putting re-enforcement (positive and negative) mechanisms in place for compliance.

[04] Van Hoye, G., & Lievens, F., Social Influences on Organisational Attractiveness: Investigating If and When Word of Mouth Matters, Journal of Applied Social Psychology, 2007.

[05] 5Jauhari, H., Singh, S., & Kumar, M., Employee Brand Building Behaviour: An Investigation of its Outcomes for the Employer, Paper presented at the 2015 Annual Conference of The Emerging Markets Conference Board held at IMT Dubai, 20-22 January 2015.

Second order risks

Brand sabotage

As per a chain of research studies[06, 07, 08], a major proportion of employees (estimated to be up to 75 per cent in some cases) indulge in active or passive brand sabotage. Studies reveal that service sabotage behaviour of employees is very common in firms.

For example, 5 to 96 per cent employees admittedly ever had dishonest behaviour in workplaces; about 69 to 80 per cent employees have demonstrated social loafing in firms; 33 per cent to 75 per cent employees had dysfunctional behaviour, such as stealing, cheating, destruction and absence in workplaces; and up to 75 per cent of employees indulge in active (saying negative things about the brand) or passive (under or over representation of a brand) brand sabotage in front of customers[06, 07, 08]. Brand sabotage by employees may have hounding consequences for a company that may not always be objectively visible. However, as per a financial estimate, a loss of over USD800, 000 was caused by service negligence every year in the late 1990s[09]. To the extent that the frontline service delivery is outsourced or partnered with other firms, the risk of sabotage is higher.

Employee branding as a strategy of creating brand engagement and aligning employees by establishing brand representation guidelines, translating brand promise delivery aspects to each role, developing employees into brand champions and building brand supportive climate is a promising avenue for exploration. Firms should invest in employee branding to avoid the risk of brand sabotage by employees and representatives.

Capability risks

Amidst the fast changing nature of work coupled with the increasing frequency of organisational changes, the concerns of scaling employee capability cannot be cornered. Talent development and change management professionals are often jostling with the challenge of making the organisational workforce future ready. Easier said than done, the ability of organisational talent to support the organisational strategy is the biggest risk for strategy execution. At a higher level, the capability of managers to deal with workplace dynamics and the capability of leaders to navigate the organisation through a dynamic environment are other areas of concern.

Risk management should take into consideration the risks pertaining to capabilities of people who are responsible for executing a strategy.

Capacity risks

Definition of a role is the starting point for defining organisational structures and manpower planning. An organisation's sizing and workforce productivity are often impacted by the way roles are defined. An improper role definition may lead to under/over utilisation of resources, inability of performing the job responsibilities appropriately, job burnout, and under/over staffing. Further, an improperly planned role may create bandwidth issues for people managers, in terms of juggling with people management and individual contribution responsibilities. Ultimately, these issues adversely impact the performance of employees and organisations.

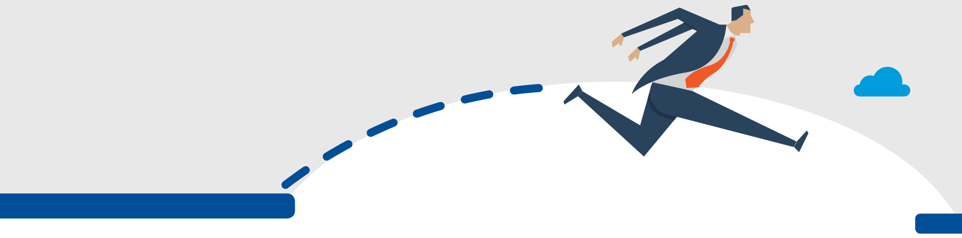
Risk management from a capacity perspective is an important area of attention. Job analysis, utilisation and productivity measurement studies and interventions knitted around them can help organisations mitigate capacity risk to a great extent.

[06] Harris, L. C., & Ogbonna, E., Exploring service sabotage: The antecedents, types and consequences of frontline, deviant, anti-service behaviours, Journal of Service Research, 2002.

[07] Harris, L. C., & Ogbonna, E., Service sabotage: A study of antecedents and consequences, Journal of the Academy of Marketing Science, 2006.

[08] Chen, C., Lei, J., & Hao, J., Hotel staff service sabotage behaviour: Classification and impact on consumer willingness to pay, International Journal of Marketing Studies, 2015.

[09] Harris, L. C., & Ogbonna, E., Service sabotage: The dark side of service dynamics, Business Horizons, 2009.



Way forward

The milieu for managing human capital risks in India is going through a slow-paced evolution. In a recent study of executives, it emerged that about 62 per cent top executives consider human capital risk as an urgent Board-level concern. About 35 per cent of organisations have formally defined risk mitigation strategies[10]. Given the seriousness of human capital risks and the complexities involved in managing them, human capital risk management surely deserves top-order attention. Due to multiple ownerships of human capital, human capital risk management should become the shared responsibility of the HR, risk and compliance functions together with the senior business leaders.

[10] Seth, M., Mitigating the human capital risks in India. People Matters, 26 May 2016.

Risks of creating an effective workforce

Introduction

An organisation's workforce profile is composed of employee groups that show differences on the basis of functional specialty, age, sexual orientation, life style, geographic origin, etc., thus leading to diversity at the workplace. Workforce diversity is a resource that adds to performance through cognitive benefits and a challenge from the perspective of workforce management[01]. Organisations are increasingly reporting challenges pertaining to management of the workforce mix from different generations (Gen X and Gen Y/millennials).

Both Gen X and millennials bring along with them their unique strengths. However, given the difference in preferences, expectations and the styles of working of these generations, it is a challenge to bring them to terms with one other. Harnessing the wave of the next-gen workforce (millennials) and integrating them with the mainstream experienced professionals (Gen X) is crucial for creating a successful and sustainable workforce operating model.

[01] Jauhari, H., & Singh, S., Perceived diversity climate and employees' organisational loyalty, Equality, Diversity and Inclusion: An International Journal, 2013.

Vishalli Dongrie

Partner

People and Change Advisory
KPMG in india

Understanding millennials

The concept of authority

Millennials do not perceive authority as a point of deference. The way this generation has been raised, they believe that their voice matters and they value individualism. They don't shy away from asking questions and believe in stating their opinions boldly. To them, positions are sets of responsibilities by the virtue of experience and expertise. In no way, do they like position holders to command and control, unnecessarily[02].

Work motivations

Millennials are motivated by a sense that what they do matters, along with the opportunity of being creative, work-life balance, career progress and development. They strive for a sense of accomplishment for making an impact at work and they want their jobs to offer them avenues of channelizing their creative energy. Millennials want to experience as much growth and targeted development as possible in the most interesting way. So, it is important to engage millennials with customised and blended development opportunities.

Technology enablement

Millennial employees are adept with technology. They are not only skilful at using technology, but they prefer using it regularly. Working the way 'it has always been done' is a spoiler for them as they try to inject updated technology and workflows. They increasingly prefer technology-enabled workplaces which help them to experiment and achieve efficiency.

Instant feedback

Millennials approach work in a fast-paced and participative manner. They prefer working on their ideas proactively and obtain instant feedback on the same. Waiting for the entire output to emerge before they could seek feedback and long cycles of iterations do not excite them. They work best with this instant cycle of prototyping, getting feedback and repeating. They view feedback mechanisms as a continuous motivation cycle and not as the end state of a positive or negative judgement.

Flexibility

Millennials need flexibility with respect to work and benefits. In terms of work, they value flexible work timings and modes of work that allow them to focus on their work, get things accomplished and then return to their daily lives. They don't want to be looped in routines and monotony. They want flexible benefits that gives them more spending power and the ability to decide what meets their individual needs as their lives change[03].

Pace of work and growth

Traditionally, career advancement is linked with seniority and the duration of service. Millennials value results over tenure and can get frustrated if it takes unreasonably long to work up the career ladder. Millennials want career advancement to be linked with capability rather than other time bound parameters. Moreover, they believe in a fast pace of work and expect fast decision-making/support systems to help them speed up.

[02] Asghar, R., Gen X is from Mars, Gen Y is from Venus: A primer on how to motivate a millennial, Forbes, 14 January 2014.

[03] Taylor, B., Millennial job search - What employee benefits are most important? About Money, 22 June 2015.

Recommendations for HR Managers

Awareness of diversity

Bringing together two generations requires an investment on building awareness about the expectations and approaches that each generation needs to follow to synchronise with the other. It's not a matter of who compromises for the other, rather how two generations imbibe flexibility in their approaches to collaborate effectively. One of the biggest reasons why diversity becomes a challenge is the lack of awareness about the ways to deal with it. From a development point of view, this is going to be imperative. Awareness building programmes can enable Gen X and millennials to better understand each other's working styles and identify flexible approaches that make collaboration among them easier.

Roles for the future workforce

With new role takers coming in, the traditional role definitions may no longer remain attractive. It is time that roles be re-designed to offer exciting avenues to millennials. The future workplace needs to be smart and facilitate seamless integration of teams and gives rise to efficiencies. Roles of the future are expected to have technology embedded in them, heightened collaboration across teams and geographies and also open more avenues for creativity.

Appealing employee value proposition

It is important for employers to explain what they are offering to millennials. It is time to think creatively about reward strategies, flexible benefits, work-life balance, and clear growth opportunities to motivate them. Additionally, the promised employee value proposition (EVP) must be tested against the reality of employee experience. All the promised benefits must be realised and not remain confined to papers/policies. The extent to which companies can minimise the gap between perception and reality, they will be able to attract millennials.

Growth and development avenues

Personal and professional goals of millennials need to be understood and a blended development approach needs to be adopted to keep them engaged. Right from challenging assignments that give them a sense that they are moving towards something significant to gamified learning, interesting ways of development need to be practiced. Organisations should challenge them to come up with new ways to streamline processes and to exercise creativity; make them a part of global assignments; make them a part of a mentoring process; and let them experience cross-functional and cross-cultural teams.

Workforce analytics

Use of analytics at the workplace is the next big thing. Insights from real time data analysis can form the base for decision-making on aspects relating to performance management, engagement, diversity management and productivity enhancement. Active application of workforce analytics can enable HR and business leaders to make more effective decisions and ultimately improve business results. People managers should be developed to understand and use analytics at the workplace, in order to practice evidence-based Human Resource Management (HRM). There is a rising trend towards the use of predictive analytics in hiring, pay for performance, diversity management and initiatives focussed on the well-being of employees.

Risk of disruption in emerging sectors

Sreedhar Prasad

Partner
Ecommerce and Start-ups
KPMG in india

Today's business environment is getting increasingly complex, volatile and unpredictable, with disruptive innovation – both in terms of products/services and business/operating models – constantly challenging the established businesses. A large portion of this technical effort is today focussed on optimization of operating models, behavioral trends, technology, social media integration and channels for customer acquisition, which the new-age businesses are leaving conventional businesses behind on each front.

New payment modes, changing social patterns, technological advancements and rising competition, all have the ability to further influence the customer – supplier relationship and create more opportunities for disruptive models to carve a niche for themselves.

While the internet enabled business models today are less likely to be significantly challenged by newer business models, they still are vulnerable to technological disruptions which can make their newer competitors more advanced and sophisticated. No one expected 'maps' as a technological medium five years ago as a business enabler. Today it is the key enabler for hyper local businesses and logistics. However, the next phase of transition may not be driven by technology alone. Given the access to customers' demographic information and purchase patterns across channels including, but not limited to: offline, website, and mobile application, behavioral patterns and social media analytics can also play a critical role.

The management, investors and Board as well as employees across levels, will have to look beyond the current challenges to anticipate such disruptions which are ambiguous at best and difficult to identify as a threat until it materializes into one.

Below are some of the current disruptive models that have the potential to alter the way business is conducted:

Business alliances

Win-Win models by totally unrelated businesses given sudden access to large customer base, and thus a huge competitive advantage. These could be an e-tailers tying up with a company having thousands of outlets or a financial services platform tying up with a ticketing company.

Integrated platforms

The concept of a platform technology is based on the belief that a single technology may not be able to solve all business problems. Platform integrations are on the rise which is leading to a seamless experience.

Payment models

Newer forms of payments have been used as powerful tools to break open certain markets by the dominant players. Be it cash on delivery in India, or credit in China, it is interesting to note that the some of the most predominant payment forms vary across countries, which can be attributed to factors like demographics, income spread and financial maturity of the nation.

Data

Protection of customer data is of prime importance to companies. With the amount of data ever growing at an exponential rate, it is crucial that companies provide security and privacy of data at every step in the process.

Internet of Things

Intelligent automation means combining technology with people to get a job done in a more efficient way or a more effective way. The Internet of Things (IoT) can change the way people interact with their business and personal ecosystems.

Risk mitigation in e-commerce

Many of the disruptions and innovations pose existential threats to e-commerce companies, and the global giants have taken significant steps to shield themselves from/adapt to these risks in many ways:

- Strong strategic alliances and business relationships to strengthen business position, expand the market, and to create entry barriers.
- Always on an innovation mode, whether on customer experience, products and channels. This helps in continually managing the risk of inability to scale.
- Investments in advanced technologies and focus on customer experience to create a trusted brand.
- Heterogeneous pool of resources for managing the day to day operations, to bring in a wider perspective for quick problem solving.
- Building an ecosystem mindset than a transaction mindset, leading to a win-win model.

The e-commerce players are expected to continue investing in areas which continue to make them more efficient and optimal each day. Given the dynamicity of the business, there are new risks which companies and their customers can be exposed to in the coming days, weeks or months. One of the best defenses for the new generation and existing companies might just be offence – to plan for being ahead of the curve and proactively adapting and innovating to ensure threats are mitigated even before they get a chance to have material impact on operations.

That being said, there will always be risks which catch companies off-guard. The unique-selling-point of e-commerce has been quick innovation and we hope they will be able to react to such disruptions effectively and ensure minimal impact on their customers, sellers and other stakeholders.

Crisis Management - preparing for the unknown

Sundar Ramaswamy

Partner
Advisory Services
KPMG in india

Steering the organisation through crisis - An organisational perspective on crisis management

Crisis management is an organisational level concept that focuses on the preparedness and response of an organisation during the face of a crisis that threatens to disrupt the day to day functioning and thereby, the business as a whole.Effective crisis management leads to coordination of an organisation's efforts to respond to a crisis in an efficient and timely manner while avoiding or minimising damage to the organisation's profitability, reputation or ability to operate. Primary objectives of a crisis management plan should involve the following rudimentary requisites:

- Setting up a Crisis Response Team (CRT)
- Defining a 'crisis' and extrapolating the various types
- Setting the goals and mission of Crisis Response Team (CRT)
- Reviewing the tasks and objectives of Crisis Response Team (CRT) – communication, asset safety, employee safety and continuity
- Assignment of roles and responsibilities of Crisis Response Team (CRT) members
- Provision of necessary information and periodic training (drills) to the employees of the organisation.

Crisis management demands the consideration of the following points to meet the level of robustness required to safeguard the technological assets, employees and the day to day functioning of the business during a crisis:

Team

The first and foremost requisite for emergency/crisis preparedness is to identify Crisis Response Team (CRT) to execute the same. Several organisations tend to identify employees who are placed in strategic positions inside the premises of the organisation to ensure appropriate action is taken without considerable buffer. Designated sub-teams are set up to meet the aforementioned objectives (communication, asset safety, employee safety and continuity).

The Crisis Response Teams (CRTs) reports to a Crisis Management Leader who holds the veto with respect to all strategic and safety decisions during the time of the crisis. A typical Crisis Management Leader in an organisation is responsible for the following:

- Availability
- Analysis of the crisis, understanding/predicting the intensity and formulating the strategy for the way forward
- Availability of a plan B
- Prioritisation of the action items in the crisis plan document depending upon the nature of crisis
- Communication of status updates to relevant stakeholders.

A robust roles and responsibilities matrix is defined to map the action items against the crisis management team members, with respect to the nature of the crisis. The matrix should contain the names of the team members along with their latest contact information. Further, maintenance of a roles and responsibilities matrix and communicating the same to employees (via mailers, flyers, handouts etc.) can help establish clarity for the employees during adverse times.

The employees should be subjected to periodic trainings and drills for two main purposes:

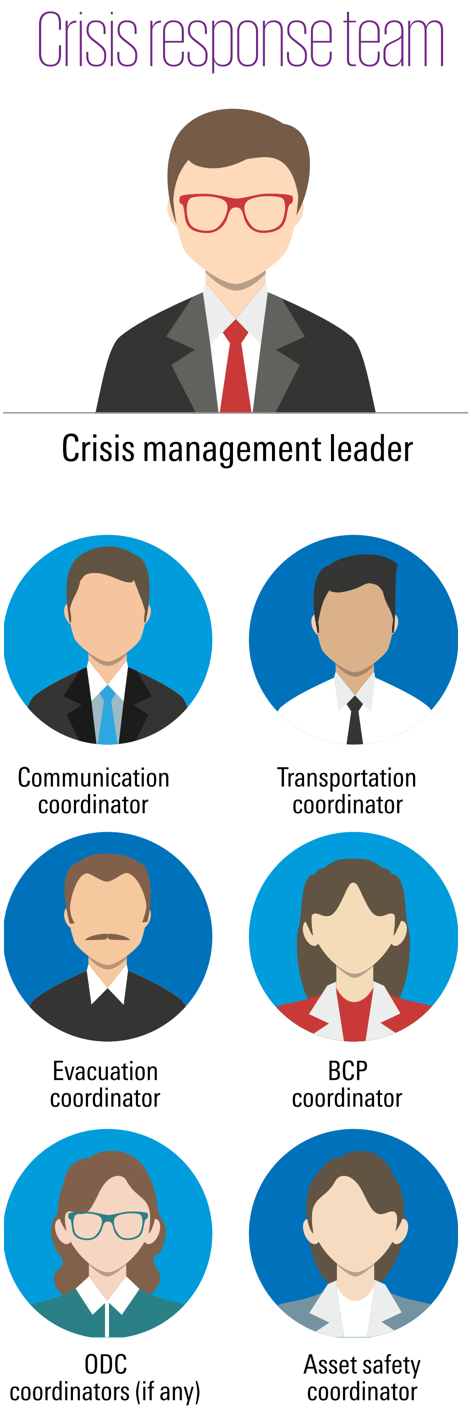
a. For understanding the steps to be followed during the time of a crisis

b. Loop holes in the action items during the execution of drills can be identified and the crisis plan document can be fine-tuned accordingly

It has been observed that while decentralised organisations foster innovation under normal circumstances, they are not suitable to handle crisis situations. A rapid centralised response is required in order to contain a crisis and this, in turn, requires a very clear line of command established where the leader has designated backup resources ready to take over his responsibilities in case he is unavailable or indisposed.

In several cases it has been observed that companies continue with their conventional decentralised structures even during times of crisis and as a result their response is rather incoherent. A central Crisis Response Team (CRT) consisting of people trained to handle such situations is absent in many cases.

A typical top-down approach (for a Crisis Response Team) in organisations can hold the following structure:



Crisis response team

Crisis management leader

Communication coordinator

Transportation coordinator

Evacuation coordinator

BCP coordinator

ODC coordinators (if any)

Asset safety coordinator

Plan

There exists a plan document that outlines how the organisation will respond to various types of crises. The crisis management plan essentially contains a blueprint of the execution and elucidates in detail, the steps to be followed and the contact details of important personnel. A few of the leading practices are as follows:

- Analyse possible crisis situation: A list of possible crisis situations that provides direction to the planning process. It is advisable to identify the emergency situations that the organisation is most susceptible to, so that crisis plan can be developed for such situations
  Examples: Earthquakes, blackouts, flooding, epidemic, bomb threats, fire, etc.
- Define modularised response options that can be applied individually or as combinations depending upon the nature of the crisis.
  Examples: facility lock down, evacuation, quarantine, relocation of resources etc.
- Lack of clarity over the roles and responsibilities can severely impact the organisations' recovery time. Crisis situations can leave key resources indisposed or unavailable. Having a clear understanding about who holds the veto when the designated person is unavailable is critical.
- Defining the business continuity objectives. The document defines critical parameters such as maximum tolerable period of disruption and Recovery Point Objective (RPO). The RPO considers how much of a company's infrastructure, whether it be data, facilities, processes or other key components, needs to be restored before operations can resume normally.
- Crisis communication plan: Another important element of the crisis management plan is the crisis communication plan which designates spokespersons, and establishes the media and PR policy. The plan should identify the internal and external stakeholders that matter to your organisation and provide standard communication templates that needs to go out to each. During crises conventional communication channels such as mobile networks and e-mail services may not be accessible. The organisation must identify alternative channels of communication by which it can reach all personnel at short notice.
- Contingency resources and backup arrangements: The plan also has to stipulate the contingency resources that are required to deal with a crisis situation. This may include office supplies, infrastructural resources, backup power, manpower as well as food, drinking water and first aid. The plan should also define the guidelines for storage and retrieval of digital data which describe where it is to be stored and how it is to be accessed in case of an incident.

While many companies have well-rehearsed plans in place for the customers as well as employees, the support service plans are not accounted for. Support functions such as administration, logistics, supply chain etc., are crucial during a crisis situation. If the support functions are not available, then the organisation may not be able to effectively follow the recommended response options.

Therefore, it is recommended that businesses accord organisational planning equal priority as business continuity plans from a customer perspective.

Further, it was also observed that most companies had failed to identify the dependencies and potential points of failure in the crisis management plan and hence faced a lot of delay in invoking them during a real time crisis situation.

Preparation

Once the crisis plan document is in place, the organisation takes necessary steps to ensure that it is prepared to handle any crisis situation according to the guidelines defined in the document. In order to accomplish this, the Crisis Management Leader assesses how prepared the organisation is to handle a crisis in its present state by conducting trainings and drills. This analysis reveals the risks, threats, vulnerabilities and the loopholes in the action plan executed. Based on the results of the trainings and drills, the Crisis Response Team (CRT), along with the Crisis Management Leader, tailor down/fine tune the action plan for various kinds of crises. The Crisis Management Leader can help ensure that the following are in place with respect to being prepared during the time of crisis:

- All the resources identified in the plan are available at any given point of time
- The channels of communication of important information to relevant stakeholders are hassle free during the time of the crisis
- Ready availability of a contingency plan for communication of information to relevant stakeholders
- Transportation facilities to move the employees from the location of crisis (the office premises) to a safer location
- A sturdy Business Continuity Plan (BCP) to work on – alternate site to operate from in the event of a crisis, to support the operation of the critical parts of the business
- Entering into contractual agreements with third parties for provision of crisis management and Business Continuity Plan (BCP) services
- Scheduling simulations and real time drills to ensure that the employees and stakeholders are aware of the course of action to be taken during a crisis.

Communication is one of the most crucial elements of crisis preparedness and the most common point of failure as well. Reaching all the stakeholders on time is a challenge that companies face even today. Organisations should devise means to dispatch messages to all the affected staff members as fast as possible. This can be done by means of social media accounts set up exclusively for this purpose through which messages can be broadcast to all the effected personnel through a single device.

Another challenge as far as communication is concerned is delivering a measured and standard response. Often it is observed that the core crisis communication team is inadequately trained to speak on behalf of an entire organisation. The spokespersons should be trained to prepare standardised messages in a way that it optimises the response of all stakeholders.

Execution

This stage involves the actual implementation of steps defined in the crisis management manual. According to the crisis situation the Crisis Response Team (CRT) identifies the appropriate response steps to be taken to ensure recovery of business operations to a pre-disaster state or at least enable the business to continue operating at a minimum acceptable level. This includes damage assessment, damage control, rescue and rehabilitation, coordinating logistics between facilities etc.

Post mortem analysis

Organisations facilitate the performance of a post-crisis review by the Crisis Response Team (CRT) after each significant crisis. This exercise can help identify the learnings that can be used for fine-tuning the existing crisis management framework and to make improvements. A post crisis review can also help us identify what worked and what didn’t work and modify the plan accordingly.

Conclusion

Organisations tend to have a documented plan and procedure for crisis management closely (if not completely) conforming to the aforementioned criterion. However, during the time of crisis, the execution might require tweaks and achieving cent percent efficiency can be difficult. Alas, the secret of crisis management is not good vs bad; it is preventing the bad from getting worse. Hence, organisations must keep fine tuning the crisis plan document at all times so that the effects are curbed to the maximum extent possible.

Globalisation and multiple tax risks

Girish Vanvari

Partner and Head
Tax
KPMG in india

> There's a justified public concern in all our countries, certainly in the UK, that multinationals are using outdated international tax laws to avoid paying a fair share of taxes in all jurisdictions.[01]
>
> George Osborne
>
> **Chancellor of the Exchequer**
> United Kingdom

Statements such as the above have become the norm, more than an exception, as global developments on the tax front grab headlines like never before. As India continues with unprecedented changes in its tax policies to boost investor confidence, the need to plug tax loopholes has equally led to introduction of anti-abuse legislations and greater disclosure requirements. Globally, the Base Erosion and Profit Shifting (BEPS) project[02] has been one of the most unified tax policy initiatives between nations which is expected to have significant impact on holding structures and business models in the global business context.

As regulators across the globe become more stringent on the compliance in law and spirit of their respective country's tax laws, the role of tax management is also evolving. Tax management has moved beyond mere compliance and minimisation of the effective tax rate, as it is also a reputational issue for global businesses. With India Inc. continuing to expand globally, the natural by-product of such expansion is increased risks. Awareness and effective management of tax risks thus becomes critical for India Inc. to maintain its global competitiveness.

Risk of PoEM

International expansion of business can be undertaken in varied forms such as branch, subsidiary, liaison office etc. However, a subsidiary company is often considered the preferred form for establishing permanent presence in a foreign country.

In terms of tax exposure, a foreign subsidiary is not taxable in India in relation to its foreign income. However, with the recent introduction of the concept of 'Place of Effective Management' (PoEM) under the Indian domestic tax laws, this position may not hold well in all scenarios.

A foreign company's place of effective management will be deemed to be in India, if its key management and commercial decisions are in substance made in India. For instance, it is very common for multinationals to operate through an Offshore Holding Company (OHC) model for investment across operating subsidiaries in various countries. Where the key management decisions of an OHC such as mode of funding of any operating subsidiary, exit strategies are being taken in India or by key management personnel in India, the risk of trigger of PoEM is high. This may result in taxation of such foreign subsidiary's income in India as well in the foreign jurisdiction (though credit of foreign taxes paid is likely).[03]

Determination of place of decision making is not a straight forward process and the government has circulated draft guidelines for determination of PoEM. The draft guidelines for instance, provide exemption to foreign subsidiaries undertaking active business outside India, subject to certain conditions. However, in sum and substance, the tests laid out in the draft guidelines are subjective and take into consideration factors such as actual decision making by the foreign subsidiary's board of directors, location of Head Office (HO), place where substantial activities are carried out etc. A proactive assessment of the decision making process for global operations, ring fencing of such decision making matrix and robust documentation from a tax audit perspective is critical to mitigate adverse tax and compliance risk due to PoEM.

PE risks

Indian entities may operate and sell goods in another country without setting up a direct presence as well. For e.g. an Indian software exporter can enter into a distribution agreement with an agent in Germany for sale of its software in lieu of commission. Typically, the profits earned by the Indian software exporter would not be taxable in Germany as it would not have a taxable presence or Permanent Establishment (PE) in Germany. Action Plan 7[04] of the BEPS project deals with preventing artificial avoidance of PE status. The changes proposed in the PE clause of tax treaties can result in tightening the agency PE rules to include contracts where such agents play the principal role leading to conclusion of contracts that are routinely concluded without material modifications.

While Indian tax authorities have always been vigilant in verifying whether there is a PE of a foreign enterprise in India, with proposed amendments to PE threshold such as above, there may be greater scrutiny of creation of PEs by foreign tax authorities as well. For instance, in 2015, the U.K. introduced diverted profits tax which is levied when a foreign company undertakes activities in the U.K. in a manner designed to avoid creation of PE, i.e. taxable presence in the U.K. In light of such developments, evaluation of existing business models of India Inc. is the key to mitigate any additional tax risks due to establishment of PE in a foreign country.

[01] http://www.ft.com/cms/s/0/82950ede-d18d-11e5-92a1-c5e23ef99c77.html

[02] The OECD commenced the BEPS project to address concerns of existing tax rules allowing multinationals opportunity for arbitraging tax rates and regimes. The final BEPS report containing 15 specific Action Plans, were ratified by the G-20 Finance Ministers at their meeting in Lima, Peru on 8 October 2015

[03] CBDT has notified the foreign tax credit rules on 27 June 2016. The rules are silent on foreign tax credit in case of PoEM of a foreign company in India.

[04] http://www.oecd.org/ctp/preventing-the-artificial-avoidance-of-permanent-establishment-status-action-7-2015-final-report-9789264241220-en.html

Offshore Holding Companies

Use of OHC structures are common for global businesses as they provide flexibility in terms of ease of exit, corporate restructuring, joint ventures, private equity funding etc. Tax efficiencies on exit and/or repatriation is also one of the key benefits where an OHC is interposed in a tax friendly jurisdiction. However, as Action Plan 6[05] of BEPS sets the guidelines for prevention of treaty shopping and treaty abuse, anti-abuse provisions such as Limitation of Benefits clause are likely to form part of tax treaties in future to limit the use of OHC's purely for the purpose of tax benefits.[06]

Therefore, while OHCs is likely to continue to exist in holding structures for the operational advantages they provide, the robustness of such OHCs in terms of substance now needs to be demonstrated for such OHCs to be entitled to any tax benefits that a bilateral tax treaty has to offer.

In the Indian context as well, the introduction of GAAR[07] provisions from April 2017 onwards will lead to increased scrutiny of arrangements whose main purpose is to obtain tax benefits.

Transfer pricing risks

Globalisation invariably brings complex intercompany transaction structures and Transfer Pricing (TP) policies into play. Increasingly, a large number of countries have adopted specific TP regulations to check abusive TP arrangements that can potentially diminish their tax bases. The Indian TP regulations have seen quantum transformation since they were introduced in 2001. Perceived as one of the most aggressive and litigation-prone TP regimes in the world, India has adopted several measures in the recent years, including Safe Harbour Rules and Advance Pricing Arrangements (APA), to provide certainty to taxpayers on TP matters. With 77 APAs[08] signed in the last 24 months and several legislative changes to streamline the TP regulation and ease the litigation process, the mind-set of the Indian government to move towards a non-adversarial tax regime is visible. However, continuing litigation in India around many complex TP issues and several BEPS-initiated developments, managing transfer pricing risks remains critical for multinationals.

With Action Plan 13[09] of the BEPS requiring country-by-country (CbC) reporting, the transfer pricing disclosure requirements globally have got elevated to unprecedented levels. Already implemented in several countries including India, the CbC reporting aims at providing tax authorities clear visibility into multinational enterprise's corporate structure and allocation of income, taxes paid and indicators of economic activities among various group entities across the globe. Applicable for multinationals with consolidated revenues in excess of EUR750 million. These new disclosure norms on TP are an action item for many. To facilitate global accessibility of the CbC information, as of 30 June 2016, 44 countries[10] (including India) have signed a Multilateral Competent Authority Agreement on Exchange of CbC report, which can facilitate automatic exchange of such information. While designed as a first-level risk assessment tool, it is suspected that CbC reporting may lead to increased tax controversy as different tax authorities may interpret the disclosures without appreciating the nature of intercompany transactions. As a consequence, greater resources may be required by multinationals to maintain such documentation as well as respond to higher levels of assessment and tax controversies.

Suspecting that misallocation of the profits generated by valuable intangibles have contributed to BEPS, the guidance under Action 8 to10 of BEPS[11] emphasises that the TP outcomes should be aligned by value creation. The proposed guidelines suggest that legal ownership of intangibles alone does not necessarily generate a right to all of the returns generated from exploitation of the intangibles. In light of such elaborate guidance, multinationals should evaluate their existing IP structures and the related TP policies.

[05] http://www.oecd.org/tax/preventing-the-granting-of-treaty-benefits-in-inappropriate-circumstances-action-6-2015-final-report-9789264241695-en.html

[06] The adoption of proposed changes as per BEPS Action Plan would involve amendments in domestic tax laws as well as tax treaties by various countries. The multilateral instrument (amending the bilateral tax treaties) would be open for signatures by all interested countries in December 2016.

[07] General Anti-Avoidance Rules

[08] Press Information Bureau release dated 18 July 2016

[09] http://www.oecd.org/ctp/beps-2015-final-reports.html

[10] https://www.oecd.org/tax/automatic-exchange/about.../CbC-MCAA-Signatories.pdf

[11] http://www.oecd.org/ctp/beps-2015-final-reports.html

Service tax risks on overseas branch transactions

In the context of indirect taxation, while supply of goods by Indian manufacturer/dealer to its overseas branch/ subsidiary is treated as 'export' of goods (and hence zero-rated), same is generally not the case for service providers in light of specific restriction in this regard.

In light of specific explanation provided in the definition of 'service'[12], as provided in the Finance Act 1994 two establishments of a person located each in the taxable and a non-taxable territory are treated as separate taxable persons. Further, service tax rules specifically provide that the benefit of 'export' of services would not be available on transactions between such persons, even if otherwise qualified.

Accordingly, while a service provided by HO in India to overseas branch can be denied the benefit of treatment as 'export' of service, a similar service by Indian company to its overseas subsidiary/holding company would qualify as 'export' of service.

On the contrary, services received by Indian HO from overseas branches are liable to service tax under reverse charge mechanism. Accordingly, remittances made by Indian head office to overseas branches for meeting routine office expenses such as salary, rental, etc. have always been contested by service tax authorities as liable to service tax under reverse charge mechanism. As regards salary payments, while one can argue that salary has been paid by HO to its employees only (which is excluded from the definition of 'service' itself) and the deeming fiction of separate taxable persons would not result such salary payments into a service payments to branch, the same could be a farfetched conjecture and subject to dispute with the authorities.

The current provision regarding 'export' of services including deeming fiction for separate taxable person have been retained in the model Goods and Services tax (GST) law[13] released in June 2016. This deeming fiction has interestingly been incorporated under the definition of 'import' of service as well by virtue of which it appears that reverse charge liability would not arise on payments made by Indian head office to overseas branches. Benefit of 'export' currently available on goods supplied to overseas branch/ subsidiary has been continued under the model GST law. Accordingly, it seems that there would be some respite to the India head offices under the proposed GST regime, if not entirely.

With the sweeping changes on the anvil in the global tax landscape, management of various tax risks shall not only be dependent on a better understanding of such developments but also how proactively an organisation is able to respond to such changes. As governments push forward with the need for greater transparency, disclosure and compliance requirements are set to rise. For India Inc. to manage its global tax affairs, it is imperative to gather holistic intelligence on international tax changes and respond to the same in a planned manner relying on tax expertise specific to a foreign jurisdiction.

[12] Section 65B(44) of the Finance Act, 1994

[13] www.finmin.nic.in/reports/ModelGSTLaw_draft.pdf

Risks in Mergers & Acquisitions and joint ventures

The last few years have seen a heightened level of Mergers and Acquisitions (M&A) as Indian companies began to accept growth through inorganic initiatives amongst their core strategic goals. Gaining recognition among the international community as credible competitors, buttressed by a liberal credit regime and combined by enhanced liquidity and credit products helped fuel this trend in India.

While the factors noted above elaborate on the merits of the M&A activity, in this chapter, we have attempted to analyse specific challenges that are faced by the companies seeking to make acquisitions in India and the measures that are important for investors (in particular global investors coming into India), which if imbibed effectively can be a gainful strategic advantage and help result in a successful deal.

Vikram Hosangady

Partner and Head
Deal Advisory
Private Equity
KPMG in india

Finding suitable targets

Sourcing a suitable target in India remains a challenge for numerous reasons, including unrealistic valuation expectations, availability of suitable targets, corporate governance, compliance issues and the target’s unwillingness to sell. The socio-political diversity that India offers along with its federal regulatory structure has resulted in several businesses adopting a regional approach to market growth and as such few true national players exist. Moreover, a large percentage of the business landscape is dominated by smaller companies that are frequently family-owned. With a few of even the most successful companies unable to achieve scale, many acquirers cannot find companies that meet their initial screening criteria.

Building a local presence in India prior to exploring M&A in the country may prove to be gainful for acquirers as India is an assorted market with several distinct characteristics. Prior to a deal, it is important for acquirers to be thorough in their knowledge of the regulatory policies as applicable in different states, varied regional market practices along with the social norms. All of this is expected to take time and should be planned, accordingly.

Another vital aspect that needs to be considered by acquirers, in particular inbound acquirers, is that many Indian companies are likely to be firmly controlled by promoter families. These promoters perceive their companies as a family legacy and therefore attach a significant amount of emotional premium to the thought of selling.

With the aforementioned reasons, acquirers should ideally plan for their presence in India well before their transactions materialise. This could be done either by forming a subsidiary in India or by developing/maintaining trade relations. Getting to know and winning the trust of the promoters and the family can be key to closing a deal smoothly.

Pricing it right

The other big challenge that acquirers face is arriving at a valuation and backing it up with a credible business plan for the business to be acquired. Highly optimistic projections remain a part of the problem along with obtaining a sensible historical baseline – this applies for many companies that fall within the mid-market segment.

Business contract terms in these companies are majorly relationship-based and are agreed verbally, in which case future commitments of such contracts are uncertain. For buyers, it becomes much more important to create their own business plan which can project realistic assumptions taking into consideration the factual potential of the business.

Acquirers also have to take a long-term view of the synergies and market growth to support the need to pay a higher deal multiple. Availability of reliable deal information on account of a relatively short M&A history in India remains a concern, as comparable multiples can then be difficult to determine. An ideal measure therefore could be to use a combination of global and Indian comparables to arrive at a range, with the final price arrived at being a negotiated figure.

In fact, as is seen in many inbound transactions, comparable multiples along with key factors such as market access premium and assumptions around synergies play a significant role in determining the final price.

Distinctive challenges during due diligence

With a marketplace so fragmented and a large percentage of targets family-owned, M&A in India presents some exceptional due diligence challenges. Sellers in India often lack the experience required in the transaction process which leads to delay in providing information on historical data and consequently in developing realistic forecasts that can be connected to past performance. Strategic acquirers/investors therefore have to develop their own business forecasts from the ‘bottom up’. This approach often leads to acquirers having to seek independent validation of future contract commitments, among other valuation inputs. Seeking connects and relationships as formed by the promoters may be vital to ensure business continuity as also using transaction structures that leave the liabilities behind.

Issues relating to compliance, tax or historical performance commonly surface during the due diligence stage and these might serve as deal breakers. Acquirers are therefore advised to be aware of any associated liabilities. It is also important to gauge the impact of significantly altering the business practices of the target company.

While acquirers need to factor adequate time for extended discussions on account of valuations and due diligence, a well-organised process with verified financial information that includes an explanation for discrepancies along with a strong business plan with adequate rationale will certainly help avert loss of momentum during negotiation.

Nailing the deal

While a thorough process in assessing valuations and during the due diligence stage are vital for a transaction, there are other areas that need to be considered while conducting a gap analysis to negotiate successful deals. These include:

- Working with sellers to create amenable deal structures that leave maximum cash in their hands
- Implementing an earn-out structure, in effect linking valuation to the future performance of the business
- Seeking a consensus from the promoters to be involved in the business for financial or personal reasons, even if for a short term
- Evaluating tax structures to reduce the quantum of tax liabilities for the seller
- Understanding potential integration risks and post-deal issues during the due diligence process, including cultural, operational, environmental and labour issues. This can help in making the transition successful
- Responding rapidly in circumstances where the target has funding issues.

While working through all these areas, a primary concern for the acquirer remains the ability to achieve a balance between ownership transitions.

Importance of managing your intellectual property

Ritesh Tiwari

Partner
Forensic Services
KPMG in india

Sumantra Mukherjee

Director
Forensic Services
KPMG in india

Intellectual property – An overview

Intellectual Properties (IP) are a collection of patents, trademarks, copyrighted works, industrial designs, geographical indications, and trade secrets – which have an monetary value because of their ability to protect technologies, products and services of the IP holder/owner.

Over the past few decades, enterprises have been shifting their focus of wealth creation from accumulating physical capital (or tangible assets) to generating intellectual capital (or intangible assets), or as Organisation for Economic Co-operation and Development (OECD) calls it, knowledge based capital.01 This shift has altered the focus of competition, which is directed towards the competitive advantage derived from knowledge-based capital.

Importance of protecting intellectual property

Intangible assets encapsulate and protect the competitive advantage conferred by innovation. This transforms into enormous value for which IP becomes the guardian. In other words, IP is a baraometer of enterpises' ability to compete on a world stage.

The darker side of this competition is espionage. According to the National Security Agency (NSA) and Commander of the U.S. Cyber Command, the loss of industrial information and intellectual property through cyber espionage has resulted in "the greatest transfer of wealth in world history".[02] The Commission on the Theft of Intellectual Property in the U.S. reported that "the scale of international theft of intellectual property is unprecedented – hundreds of billions of dollars per year, on the order of the size of the U.S. exports to Asia.[03]

Challenges in protecting IP

A core proxy to identify the value of intellectual property is the cost of innovation. The process of innovation generates different types of IP, and only a portion of it gets captured in the product value. Such IP can be classified as 'protectable IP' as they are protected by different IP legislations.

However, it is equally critical for enterprises to capture and manage other intellectual property related information generated during innovation that do not enjoy statutory protection. Such information can be classified as 'unprotected IP'. Lack of adequate measures to manage unprotected IP may result in loss of commercial value associated with critical information, and potentially render the enterprises susceptible to lose out on the competitive advantage conferred by their innovations.

An illustration on the different types of protected and unprotected IP is provided below:

[01] New Sources of Growth: Key Analyses and Policy conclusions – Synthesis report (2013)

[02] Josh Rogin, "NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history', Foreign policy The Cable

[03] National Bureau of Asian Research, Report on the Commission on the Theft of Intellectual Property

Managing your IP

Threat actors target unprotected IP for a variety of economic reasons (e.g., profitability and market share) and non-economic (e.g., increase influence, advance social causes). An illustration of the same is provided in the figure below:

Risks of intellectual property

Assets

- Product information
- R&D information
- Unique business methods
- IT information

Threats

- Malicious insiders
- Rogue nation states
- Hacktivists
- Competitors

Vulnerabilities

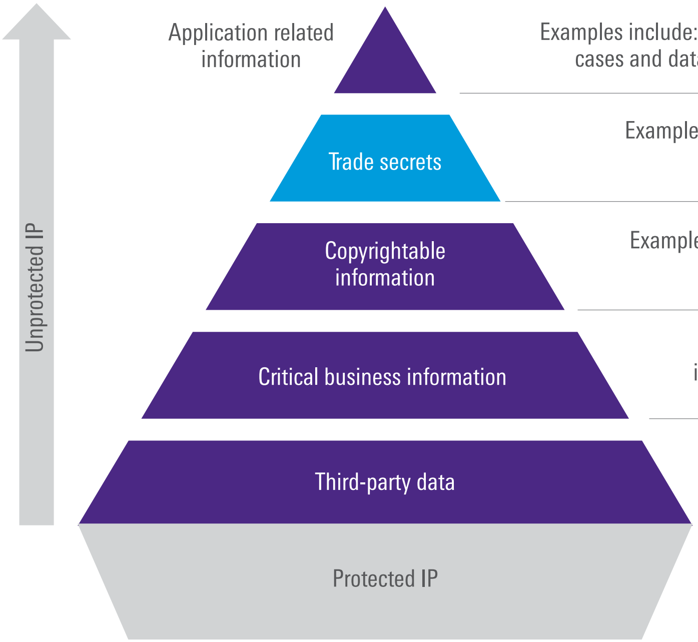
- Process gaps
- Supplier gaps
- Contract management
- Employee awareness
- IT and IS gaps

Source: KPMG in India's analysis, 2016

It is important for enterprises to adopt a risk based framework which allows enterprises to capture, maintain, and manage their unprotected IP. This is crucial since the onus is on the enterprise to demonstrate measures which can be qualified as 'reasonable care' to preserve and protect the confidentiality of such information. The duty of reasonable care requires enterprises to adopt a strategic roadmap which is a combination of administrative, process-related, and technological measures to safeguard and protect their unprotected IP.

Categories of Intellectual property

A lot of IP goes unprotected which may result in loss of critical information with significant commercial value. Such information may not be protected legally until and unless ‘reasonable measures’ are in place to protect such information



Unprotected IP

Application related information

Examples include: high-level design documents, detailed design documents, test cases and data, use cases, encryption details ,and configuration information

Trade secrets

Examples include: Algorithms, new product/solutions, and customised frameworks

Copyrightable information

Examples include: GUI, portal design, and performance improvements/ enhancements

Critical business information

Examples include: Corporate strategy, supplier information, inventory information, and personnel and financial information

Third-party data

Examples include: employee data, client data, and third-party information collected

Protected IP

Examples include: Trademarks and patentable ideas

Source: KPMG in India’s analysis, 2016

Select case studies

Case scenario	Threats	Vulnerabilities
An employee was found guilty of stealing tradesecrets associated with hybrid technology worth USD40 million	Malicious insider	Employee awareness and IS breach
An employee was accused of stealing 100,000 files containing source code for a proprietary electronic trading platform. They were valued between USD50 million and USD100 million, and was let off by the courts due to clarity of IP clauses in the employment agreements	Malicious insider	Contract management
A chemical company is alleged to have offered employment to employees of its rival as consultants to have them reveal confidential R&D information worth USD225 million	Competitors	Process gaps Contract management
A hacker group leaked a release of confidential data (employee information, salary information, and copies of then-unreleased films) of an entertainment group. This was done in retaliation to a controversial movie produced by the group.	Rogue nation state/Hacktivists	Process gaps IS breach

Regulatory and compliance risk

Ignorance is not bliss

The business environment is rapidly changing with physical boundaries no longer acting as constraints in conducting business. Rapid improvements in technology are changing business models.

These trends are creating tremendous pressure on business processes and a company's ability to manage risks effectively. To ensure strong controls in a changing business environment, an organisation's response to regulatory and compliance risk should not remain static.

As business requirements change, so do the risks as well as the organisation's response towards these risks. Structured risk management drives business value by achieving a balance between the risk management activity and business improvement. This structure also provides assurance to the management that the controls are efficient enough to identify and mitigate material risks faced by the organisation.

These risks not only include strategic, operational and financial risks but also regulatory and compliance risks, which the companies face as a result of the rapidly changing regulations that have changed as a response to the changing business environment.

Purushothaman K G

Partner

Governance Risk and
Compliance Services
KPMG in india

What has changed?

Large financial frauds and scams have compelled governments across the world to provide a mandate to corporates to adopt governance and financial oversight, integrity related principles and processes. Examples include the U.S. Sarbanes Oxley Act, 2002 (SOX), U.S. Financial Reporting Guidelines, etc. Similarly in India, the Companies Act, 2013 now requires directors responsible for developing systems to ensure compliance with the provisions of all applicable laws and assuring that such systems are adequate and operating effectively throughout the year (Section 134 of the Companies Act, 2013).

The Companies Act, 2013 also requires Directors and audit committees (Section 177) to assert and evaluate the adequacy and effectiveness of internal financial controls, which have been defined to include both operational and financial controls.

Further, Section 143(3) of the Companies Act, 2013 requires statutory auditors to mandatorily report on the adequacy and effective operation of internal financial controls (i.e. internal controls over financial reporting).

Also, Regulation 17(3) of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 stipulates that the board of directors shall periodically review compliance reports pertaining to all laws applicable to the listed entity, prepared by the listed entity as well as steps taken by the listed entity to rectify instances of non-compliances.

Non-compliance to the requirements can result in a class action suit against directors and officers and increased reputation risk.

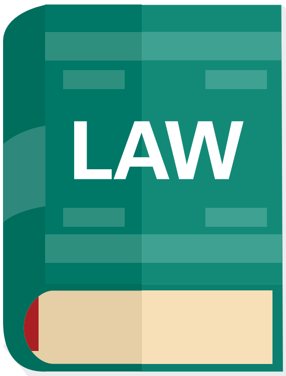
Therefore, in the light of new provisions a framework is required, which ensures that all applicable laws are identified, complied with and monitored adequately by directors and the board.

It is important that corporates select and align their processes to globally accepted internal controls framework and compliance framework, which best suit their need.

Risks perceived by organisations today

Regulatory pressures from multiple jurisdictional authorities, combined with complex organisational structures, pose challenges for organisations to holistically evaluate and report on their adherence to compliance requirements. The risks and challenges are further aggravated for corporates that have operations across multiple geographical locations with multiple legal entities and business units.

Fragmented, incomplete reporting, insufficient documentation of actions taken to address the regulatory changes and requirements and inadequate management controls can prove costly for the company.



Key threats faced due to non-compliance of regulatory requirements are listed below:

- Cancellation of licence to operate
- Loss of reputation
- Class action suit against Directors and officers, which may extend to imprisonment
- Imposition of penalties and fines
- Withdrawal of fiscal benefits
- Drop in confidence levels of stakeholders and regulators raising questions on the company’s integrity
- Increase in government and regulatory audits
- Inability to obtain new licences, which may impact business plan and strategy.

In order to move beyond the current state, organisations need to rethink or build upon their compliance approach and develop a robust all-encompassing framework to mitigate the aforementioned risks and address the challenges perceived.

The response

Increasing levels of regulation demand a greater focus on legal and regulatory compliance. Review of the existing compliance environment across several organisations has revealed that the existing compliance structures are fragmented and have not evolved with the changing business conditions. Monitoring capacities have also been incapable of answering the key requirement desired from the compliance structure – managing compliance risks to achieve the organisation's objectives. Recent experience has shown that even those companies that appeared well-capitalised and risk aware have been subject to regulatory censure.

Companies need to embrace the strategy, culture and people of the organisation while structuring or re-structuring their compliance functions to respond to the new challenges. Along with the composition of the compliance functions, the overall risk management framework should be deliberated and developed. Adoption of a robust framework provides companies an opportunity to enhance their existing governance practices. Corporates should be able to define, document and demonstrate to their stakeholders the effective governance practices followed by their organisations. In order to meet the growing regulatory requirements, the management needs to consider the following key points for developing an effective framework to mitigate and monitor the risks they face:

- Adopt a top-down approach to facilitate initiation of a compliance culture, allocation of resources and a centralised approach to address both macro and micro regulatory demands and to also provide greater strategic awareness and benefits.
- Review existing governance, internal controls and compliance framework practices in the company to identify areas which require immediate attention.
- Develop a thorough centralised global inventory of the regulatory and compliance obligations of the company. These can be linked to the respective jurisdiction, legal entity, business line, product and service.
- Conduct a gap analysis of the current compliance obligations with those required and develop an action plan to cover the risks.
- Determine the extent, appropriateness and effectiveness of current control and compliance mechanisms.
- Review the existing internal and external sources and those required to achieve the desired levels of efficiency and effectiveness.
- Develop clear accountability by establishing ownership of the risk and compliance requirements across the organisation. Mapping of operating processes/ sub-process and activities at an organisation level to its process owners and defining clear workflows.
- Develop risk policies, which reflect the regulatory environment of the organisation, mitigating the regulatory risks it is exposed to through its operations.
- Create a transition team with the appropriate authority, skill set and knowledge to execute the transition to the (re)-structured compliance framework.
- Clear communication of the company's commitment to maintain effective control and compliance framework and expectations from employees to fulfil their roles and obligations. Conduct training sessions to achieve positive compliance behaviour.
- Develop an effective compliance Management Information System to enable senior management to assess the compliance risks to which the organisation is exposed to, actions taken to mitigate the risk and the financial implications. Use of executive-level dashboards to meet requirements of Directors and the audit committee.
- Create an effective reporting, monitoring and escalation framework to provide the desired level of assertion to the higher management.
- Develop a continuous evaluation process, which checks and validates the operating effectiveness of control and compliance framework on a periodic basis.

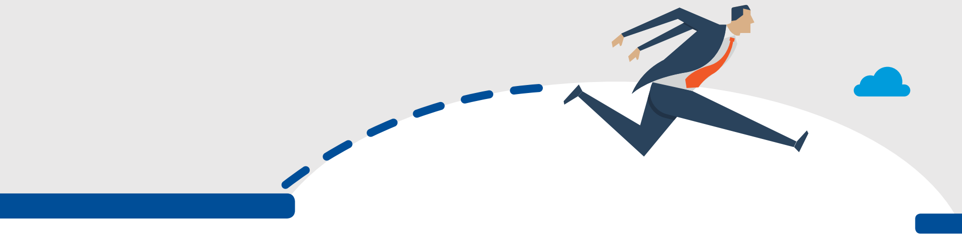
Use of technology

The complexity of the current regulatory environment, its impact on an organisation and the penalties for non-compliance cannot be addressed without suitable policies and technology to judiciously automate and manage the compliance requirements.

Compliance programmes generate a large amount of data. In the absence of a well-formulated methodology, organisations may not be able to derive value from the data generated. Appropriate technology, when managed advantageously with process and information, can help organisations monitor their compliance requirements and significantly reduce regulatory burden in terms of cost, risk and time.

Compliance tools are available in the market, which enable corporates to manage, monitor and report on regulatory compliance through pro-active e-mail alerts, management of contract and licence renewals, exception reports, detailed dashboards and action plan tracking. These tools aim to enable organisations to manage their corporate compliance programmes, such as generation of compliance certificates or delivering training programmes more effectively.

As demonstrated, the use of technology eliminates the probability of human error and reduces an organisation's risk of regulatory non-compliance by changing the compliance requirements into an effective business tool.



Potential benefits

Apart from the clear advantage of avoiding legal and regulatory penalties and complications, effective regulatory and compliance risk management can enable companies in realising the following potential benefits:

- Improved strategic decision-making due to the ability to identify the risks and costs of doing business in different jurisdictions.
- Increased visibility into the company's processes along with increased business process efficiency.
- More transparency and clearer accountability.
- Reduction of surprises faced by organisations due to clear ownership of controls and a better understanding of inherent and residual control risks.
- Possibility to use effective regulatory and compliance risk management as a differentiator in the market by infusing confidence in existing and prospective customers or stakeholders.

Large organisations can use the opportunity to assess their control and compliance environment, reduce unnecessary/ redundant controls, automate controls and update process documents covering various processes.

Conclusion

With increasing regulatory and compliance requirements, the relative cost of compliance is expected to increase, which may have a huge impact on small and medium corporates. The objective of Indian companies should be to drive their efforts towards adopting the right approach to leverage their compliance costs to drive benefits for companies and its stakeholders. Organisations need not sacrifice business improvement in order to achieve effective compliance. An organisation that balances both the goals in an integrated fashion can achieve sustained business improvement without compromising on regulatory requirements.

As the compliance journey continues, corporates can start moving from a project based approach and re-evaluate how they do business. Robust mechanisms and compliance with various regulatory requirements has compelled various organisations to develop a centralised information repository by accumulating a vast array of information pertaining to compliance, risks, controls, processes and systems. This repository has enabled business leaders, Directors and audit committees in addressing the compliance issues faced by their organisation and focussing on improving transparency in business management and boosting investor /market confidence that emphasises on business improvement with risk and controls.

Managing risks in the banking ecosystem

Minaar Malse

Partner

Governance Risk and
Compliance Services
KPMG in india

Background

India's banking and financial sector is expanding rapidly, according to the KPMG in India-CII report on 'Indian banking – Manuvering through turbulence: emerging strategies', India has the potential to become the world's fifth largest banking industry by 2020 and the third largest by 2025.

The banking industry in India has witnessed an overhaul in the recent past in terms of digital banking, innovation in the payments space and increase in the usage of technology-based alternate delivery channels.

Factors such as enhanced mobile and internet penetration, various financial inclusion measures and the expanding reach of the banking network have all contributed to innovation in banking products.

On the other hand, various challenges such as asset quality, capital adequacy, an enhanced regulatory framework coupled with competition from emerging players in the industry are impacting the banking sector.

In this context, it is important for the banks to understand how these new developments will impact them, what additional risks will they give rise to and how to successfully mitigate them.

This chapter aims to answer the following key questions:

- What are the emerging trends in the banking industry?
- What are the emerging risks in the context of new trends and challenges?
- How do these risks impact the banking industry?
- How far have the recent regulatory developments been successful in managing these risks and in bringing about transparency?

Emerging trends in the banking industry

New delivery channels and customer experience

Internet and mobile application-based banking

The past decade has seen a multifold increase in the usage of internet/mobile application-based banking facilities. This delivery channel has drastically reduced the usage of cash for transactions, reduced the need of the customer to visit the branch and enhanced their experience.

New developments in payments

The payments space has also seen multiple changes which include the following:

- Increased usage of mobile wallets for internet-based payments
- Use of Near Field Communication (NFC) technology for contactless payments
- Blockchain technology.

The mobile payments industry in India is expected to reach USD1.15 billion by the end of 2016, growing from USD86 million in 2011, clocking a CAGR of 68 per cent[01]. Additionally the mobile wallet industry is poised to reach USD183 million by 2019.[02]

Peer-to-Peer lending space

India has seen the emergence of a few start-ups in the Peer-to-Peer (P2P) lending space as well in the areas of microfinance, consumer and commercial loans. The Reserve Bank of India recently released a consultation paper on the P2P lending business model and discussed the proposed regulatory framework for these entities.[03]

Financial inclusion

In the financial inclusion space, the following key developments have taken place:

Pradhan Mantri Jan Dhan Yojana (PMJDY)

The PMJDY was introduced by the Prime Minister on 15 August 2014 to ensure access to various financial services to the excluded sections i.e. the weaker sections and low income groups of the society.[04]

The objective of PMJDY is to develop an integrated approach to ensure comprehensive financial inclusion of all households in the country. Under the PMJDY scheme, all banks, on an aggregate basis, have opened 22.48 crore accounts with aggregate deposits of more than INR 40,000 crore. Similarly, 9.46 crore Suraksha Bima Policies and 2.98 crore Jeevan Jyothi Bima Policies are issued under the scheme.[04]

[01] http://www.economist.com/sites/default/files/20150509_intl_banking.pdf

[02] http://www.ovum.com/press_releases/global-mobile-proximity-payment-users-to-surpass-1-billion-by-2019/

[03] https://rbidocs.rbi.org.in/rdocs/Content/PDFs/CPERR280420162D5F13C3A2204F4FB6A2BEA7363D0031.PDF

[04] http://www.pmjdy.gov.in/

Licensing of payments and small finance banks

The RBI issued guidelines for licensing of payments and small finance banks in November 2014 with an aim to further promote financial inclusion by providing small savings accounts and payments/remittance services and supply of credit to small business units; small and marginal farmers; micro, small industries; and unorganised sector entities.[05]

Further to the above guidelines, the RBI issued in-principle licenses to 11 payment banks and 10 small finance banks in September 2015.[06]

Regulatory environment

Comprehensive guidelines on prepaid instruments and mobile banking

The RBI's guidelines on regulating prepaid instruments and mobile banking channels coupled with the introduction of Immediate Payment Services (IMPS) by National Payments Corporation of India (NPCI) has enabled growth in their utilisation.

Licensing guidelines for payments and small finance banks

The in-principle approval provided to 11 Payment Banks and 10 Small Finance Banks is expected to contribute towards financial inclusion.[06]

Framework to revitalise distressed assets

The RBI has introduced multiple guidelines on revitalising stressed assets, including:

- Sale of assets to asset reconstruction companies[07]
- Restructuring guidelines for long-term project loans[07]
- Formation of joint lending forums[07]
- Strategic debt restructuring[08]
- Flexible structuring of long-term project finance loans[07]
- Scheme for sustainable structuring of stressed assets[09].

Asset quality reviews

The RBI encouraged banks to proactively classify assets as non-performing and prepare themselves for future possibility or weakness arising by way of enhanced provisioning.

Enhanced corporate governance standards

The companies act, 2013 (2013 Act) places significant importance on enhancing corporate governance standards through a variety of measures mentioned below:

- Rigour on increased reporting framework
- Higher auditor accountability
- Easing the restructuring of companies
- Onerous responsibility on the board, independent directors, audit committee and key managerial personnel
- Push on Corporate Social Responsibility (CSR)
- Emphasis on investor protection.

One of the major themes of the 2013 Act is reporting by directors and auditors on the internal financial control framework of the entity.

Emerging risks in the context of recent trends in the banking industry

Major risks that are generally perceived by bankers include:

Credit risk

The Indian banking system has seen significant increase in the stressed and non-performing accounts in the past decade.

Business risk

The advent of non-banking players in the mobile wallet industry, P2P lending space and RBI's issue of in-principal licenses is likely to pose a threat to universal banks.

Know Your Customer /money laundering risk

Financial inclusion schemes of the government, such as PMJDY, has given rise to Know Your Customer (KYC) risks. Similarly, the emergence of mobile wallets, blockchain technologies and P2P entities can give rise to money laundering risks.

Operational risk

Innovative products being introduced by new entrants and their lack of experience in the banking industry could give rise to significant operational risks for these entities.

Information Technology risk

Increased usage of mobile banking, digital wallets and emergence of blockchain technology in the payments space and P2P lending can give rise to enhanced IT risks.

Compliance risk

Increased regulations in the areas of asset quality and corporate governance has given rise to multiple regulatory obligations to banking entities.

[05] https://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=32614

[06] https://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=35010

[07] https://rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=9908

[08] https://rbi.org.in/scripts/NotificationUser.aspx?Id=10293&Mode=0

[09] https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10446&Mode=0

Impact of the recent regulations introduced by RBI and Companies Act, 2013

Has increased regulation brought about better governance and the required level of transparency?

Impact of Internal Financial Controls (IFC) regulations on governance and transparency

The potential benefits which companies can realise by implementing a formalised control framework are as follows:

- Enhance the controls framework
- Define clear accountability and transparency
- Control automation
- Control over spreadsheets
- Avoid surprises
- Streamline/standardise controls
- Plug leakages/potential frauds
- Control fraud risk.

By assigning specific responsibilities to the board, the Companies Act, 2013 (the Act) has made it mandatory for those charged with governance to put in place a framework that is appropriately designed, considering the nature of business and the risks that the company is exposed to, such that it operates effectively to provide the required assurance to all stakeholders.

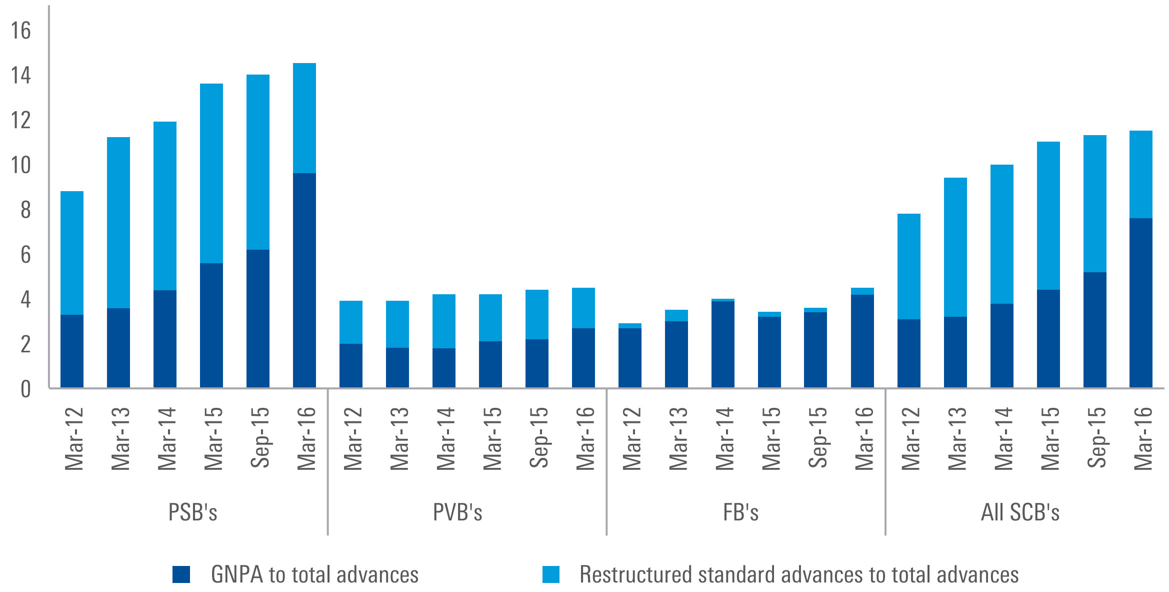
The Act has also mandated various disclosures by the Board, independent Directors, key managerial personnel and the auditors, thus enabling clear accountability and transparency.

Impact of RBI's Asset Quality Review on transparency

The RBI conducted an Asset Quality Review (AQR) with an aim to proactively identify non-performing loans and make enhanced provisioning against the same.

As per the RBI's Financial Stability Report published in June 2016, the gross NPAs of all scheduled commercial banks sharply increased to 7.6 per cent of gross advances from 5.1 per cent between September 2015 and March 2016 after the AQR.[10]

Asset quality of SCB's



The chart above shows the extent of increase in gross NPA after AQR, as this exercise has forced banks to recognise NPAs and make provisions in their books accordingly. It is important for the audit committees and the management of banks to take note of RBI's observations and proactively recognise non-performing loans and make suitable provisions to safeguard against them.

[10] https://rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=849

Impact of Central Registries on Stressed Assets, Collateral Management and KYC on transparency

The following registries have been set-up to enable banks to disclose a variety of information relating to borrowers and utilise the same for the purpose of conducting due diligence:

Central Repository of Information on Large Credits (CRILC)

The objective of setting up this registry is to collate information relating to stressed assets in the banking industry and enable the RBI to assess asset quality and uniformity in asset classification amongst banks as well as information sharing among various lenders.

Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI)

An immovable asset registry under the aegis of CERSAI has been operational since 2011. Recently, CERSAI has also been entrusted with the responsibility of supporting a robust movable asset registry. The objective is to enable banks in identifying the collaterals mortgaged to various lenders, thus avoiding the possibility of multiple financing for the same asset.

KYC registry

The CERSAI was authorised to perform the function of the central KYC registry. The objective of the registry is to receive, store, safeguard and retrieve KYC records of a client in its digital form. The same has been operationalised recently by the RBI and the live run has commenced from July 2016.

The various registries mentioned above help banks in effective sharing of information within the banking system to enable appropriate due diligence of clients for on boarding and credit appraisal and thus bringing in more transparency.

Conclusion

While the changes taking place in the banking industry are welcome on the front of technology innovation, digital banking, enhanced customer experience and financial inclusion, it is also important for the banks and regulators to recognise the risks that are emerging due to these changes.

While various measures have been taken by regulators to mitigate the critical challenges discussed in this chapter, it needs to be understood that the current environment is dynamic in terms of new entrants in the industry and innovation in products and services through technology. Accordingly, it is vital for each bank to conduct an internal assessment and arrive at customised sustainable mitigation strategies.

Each bank needs to have a comprehensive risk management framework covering the following key elements to enable them in suitably mitigating the emerging risks:

- Dynamic risk assessment framework to continuously identify the emerging risks
- Robust early warning mechanism to alert the management on significant issues at an early stage
- Strong change management framework to stay current and upbeat with the emerging trends.

Further, it is important for banks to put in place a risk management framework to not only mitigate pillar 1 risks such as credit, market and operational, but also have a framework to deal with other significant risks such as strategic/business risk, compliance risk, reputation risk, etc. to enable them to stay competitive with the changes in the banking environment.

The way in which the changes are managed will be critical in building a strong banking ecosystem.

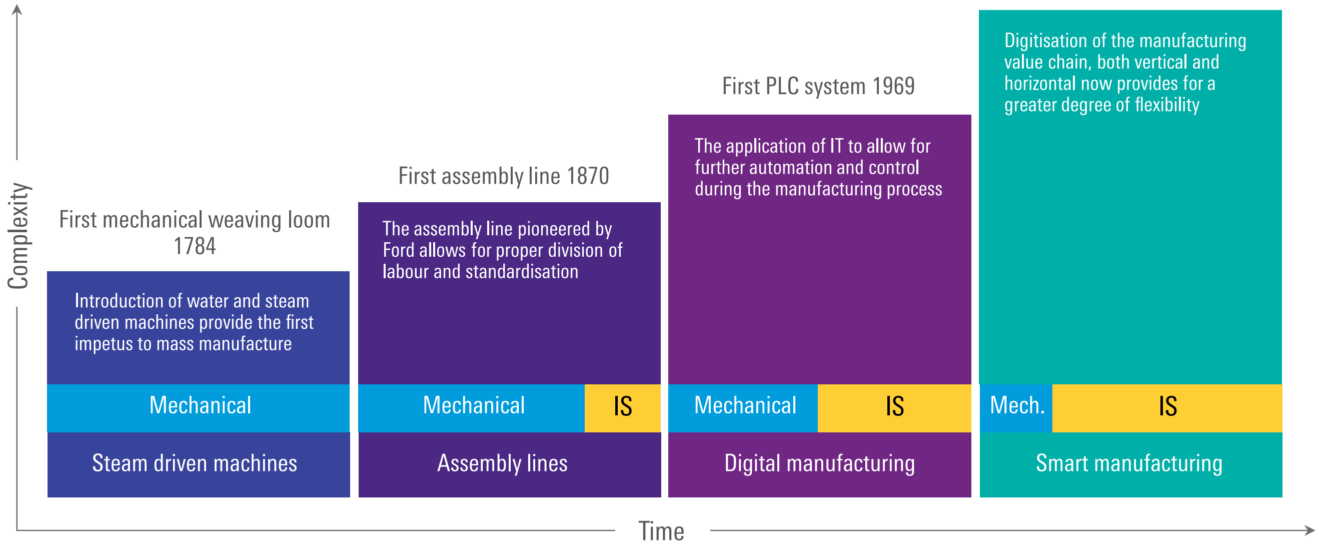
SMART systems and IoT risk for manufacturing industry

Vijay S
Partner
IT Advisory Services
KPMG in india

Merril Cherian
Director
IT Advisory Services
KPMG in india

The fourth industrial revolution is underway and for the first time it has nothing to do with physical manufacturing processes. Rarely does anything change the face of how things are made, as this revolution is expected to. In fact, the last time this happened was during the 1960's when digital manufacturing made its appearance. It is possible to identify three such turning points in the history of manufacturing, each leading to a different industrial revolution prior to the present one. (Figure 1)

1. The four industrial revolutions

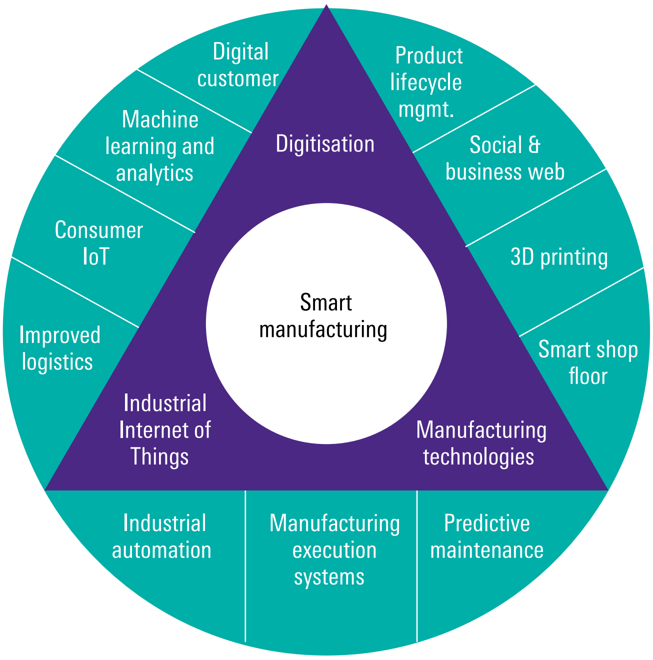


Complexity
Time
First mechanical weaving loom 1784
Introduction of water and steam driven machines provide the first impetus to mass manufacture
Mechanical
Steam driven machines
First assembly line 1870
The assembly line pioneered by Ford allows for proper division of labour and standardisation
Mechanical
IS
Assembly lines
First PLC system 1969
The application of IT to allow for further automation and control during the manufacturing process
Mechanical
IS
Digital manufacturing
Digitisation of the manufacturing value chain, both vertical and horizontal now provides for a greater degree of flexibility
Mech.
IS
Smart manufacturing

While each of these industrial revolutions changed the way in which goods are produced, the one constant has been the growing influence that Information Systems (IS) has played in the overall manufacturing process. This has led to growing complexity in the overall manufacturing process culminating in the 'smart manufacturing' era that we find ourselves in today.

Simply put, smart manufacturing involves using disruptive technologies such as Digital Automation (DA), Autonomous Mobility (AM) and Artificial Intelligence (AI) to turn the manufacturing ecosystem into a large and federated information system. This information system allows manufacturers to bring about a change in the way they deal with supply chains, the manufacturing process itself, transportation systems and labour skills. (Figure 2)

2. Smart manufacturing landscape



The 'smart' part derives from the use of various sensors, information software, data analytics embedded in the manufacturing equipment to manage both the machine's performance and the overall manufacturing process. The underpinning technologies include:

- Sensors that allow for machine to machine communication and networking – Industrial Internet of Things (IIoT)
- Software programmes that perform analytics and are able to implement machine learning
- The use of automation and robotics to perform manufacturing processes accurately and efficiently
- Augmented reality to perform quality checks on finished goods or maintenance activities on machinery
- Newer manufacturing processes such as 3D printing.

The benefits derived from smart manufacturing reflect the 'interconnected' nature of the framework. An obvious one is the ability to improve manufacturing asset utilisation. In many cases, they are also able to predict equipment failure and hence improve the maintenance process. However, one of the biggest advantages of the framework is the tight integration to other enterprise class systems (such as ERP, CRM and SCM) to better align manufacturing with the customer demand and the ability of suppliers to service these. Smart manufacturing also improves the method of manufacturing – allowing for more efficient, accurate and cheaper products. In fact, many machines within the smart manufacturing framework usually follow tighter control of the operating environment – better alignment to the optimum air, water, energy and other consumable requirements, all of which makes factories safer and sustainable.

All this is possible due to the ability of the internal sensors within the machines to generate data which is then transmitted through various company systems allowing for software analytics programmes to derive insights and actions. However, the other side of this paradigm shift in manufacturing is the changing risk landscape. As new risk exposures are created, some of the obvious risks – such as worker injuries, reduce; other newer ones such as the exposure of manufacturing systems to cyber-attack, increase. This chapter focusses on some of the key risks that the confluence of technology, networking and sensors bring to the fore.

> The very interconnected nature of the smart manufacturing framework changes the risks that businesses are exposed to – reducing some, and increasing others.

Susceptibility to cyber risk

Environments that were earlier the province of engineers with dirty and oil stained overalls have started becoming the hunting ground of suave internet warriors. The discovery of the Stuxnet worm[01] within factory systems around half a decade ago helped ensure that the risk of external sabotage of critical manufacturing environments remain at the top of mind for plant managers worldwide.

The difference now, however, is that the extensive connectivity between devices, processes and the computing facilities mean that a system failure anywhere in the ecosystem may lead to larger losses downstream. A large number of interconnected sensors have opened up the manufacturing floor to attack from outside of the enterprise. Additionally, manufacturing IT systems were generally lesser protected due to a false sense of security. After all, the assumption was that these networks were deep in the plant and not connected in any way to the outside world. These assumptions are being turned on its head with the advent of the hyper connected smart manufacturing.

Risk parameter	Value
Time horizon	Now
Impact of threat	Medium
Difficulty to fix	Medium
To be fixed	Designers, plant management

[01] The Stuxnet worm, a 500KB segment of computer code, was first identified in June 2010 at 14 plants associated with Iran's nuclear power programme

Protecting and utilising the data flow effectively

The sheer volume of data that is generated and transmitted within the smart manufacturing framework is only increasing. This is driven by the reducing the cost of both sensors used to generate the data and the computing power required to analyse the data so generated. Better networking technology is leading to additional machines and units coming online. The large amount of data currently available leads to a new situation for plant managers – for the first time they have the ability to generate near real time, actionable information about the manufacturing process; however, their IT team does not have the processes, nor the skills to do this for them.

Increasingly, plant managers are looking to outsource the analytical aspects of the data generated during the manufacturing process to service providers having specialist knowledge on the subject. The risk and impact of data theft, is likely to increase given the sensitive nature of the data being shared. Intellectual property including manufacturing design/process blueprints and performance data of the process – such as yield, efficiency and performance data now needs to be effectively protected, lest it fall in the hands of a competitor. At the same time, the protection should be flexible enough to allow for the sharing of such information and not negate the use of such data by legitimate departments in order to gain competitive advantage. As the corporate side of manufacturing learnt, securing data is a very expensive proposition if not planned for during the implementation stage.

Risk parameter	Value
Time horizon	Short term
Impact of threat	High
Difficulty to fix	Medium
To be fixed	Service providers, plant management

Setting-up for failure

Smart manufacturing lends itself very well to an apocalyptic doomsday scenario of factories run entirely by smart machines and computers. Such systems would need to be highly resistant to failure and indeed even today many of them are. However they are, by no means, infallible. When an availability issue crops up in such set-ups, there is the risk of not having anyone around with the skills to address the situation. The confluence of skills required across the manufacturing process, information technology, embedded systems and networking mean that this is a very real danger in the smart manufacturing scenario.

Increasingly manufacturers are beginning to compete with mainstream IT product/service companies for talent. This increased competition inevitably leads to the ever increasing pay cheques for competent professionals. This brings us to another risk exposure - that of financial payback. Sure, the benefits around the adoption of smart manufacturing are great, but many manufacturers are beginning to question the return on investment. If the investment in technology is made, will they have the availability of skilled resources to run it? Manufacturers are being asked to shift reliance from proven physical/electronic equipment and components to software based manufacturing control. The risks of availability and maintainability of these approaches start taking centre stage.

The deeply integrated nature of production within the Smart Manufacturing framework would entail that any impact/stoppage would be more severe and hence wider ranging than in the 'old days'. The financial impacts to the business and society are too large to be ignored.

Risk parameter	Value
Time horizon	Short term
Impact of threat	High
Difficulty to fix	Medium
To be fixed	Designers, service providers, plant management

The digital workforce

As discussed above, the skills and indeed the number of workers required to run a smart manufacturing set-up are changing. The altering pattern of labour demand does have an implication for the society as a whole. Once again, the advent of automation in manufacturing is leading to large scale reduction in the traditional labour workforce. At the same time, an increase in the technical, non-labour workforce is rarely commensurate with the loss of numbers of the former. The possibility of rising income inequality and social tensions will only increase if the labour displaced cannot be gainfully re-absorbed.

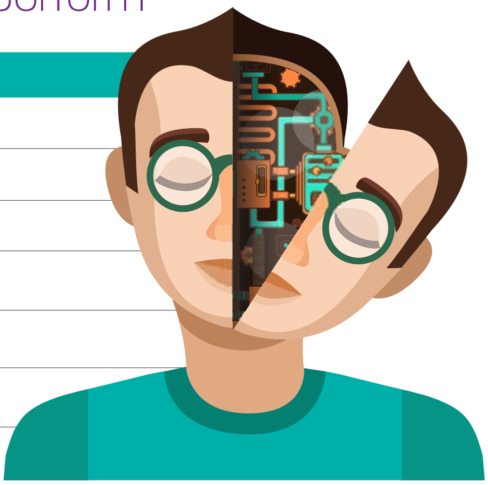
However, there is a more subtle human aspect to be examined within the smart manufacturing construct. In a framework where machines make many decisions, who makes sure that the machine makes the right decision? And where does the liability of a wrong decision finally lie? Isaac Asimov, the renowned science fiction author conceptualised a future where any robot or thinking machine must obey his Three Laws of Robotics[02] - the first of which, and also the most important one, forbade robots from putting humans to harm. However, a common theme in his writing was that of machines who realise that their behaviour or activity both upholds and violates this law, something that they are not able to manage and thereby become inoperable. Smart manufacturing requires increasingly powerful computers to create sophisticated logical systems. We may succeed in making those systems more often resemble human thinking, but that is where the semblance ends. Human judgement works due to our using values that we can empathise with which are based on real life experiences that we relate to.

Machines however, are not 'alive' and do not form values. So, they cannot make judgements – they behave based on algorithms we provide them with and, to that extent, their mistakes, however grave, are ours – for now. But this will change due to the increasing amounts of computing power at our disposal and the growing ability of machines to self-replicate[03]. (Figure 3) The increasingly autonomous nature of machinery will mean that they make decisions or judgements if you may. We are already seeing incidents where decisions made by autonomous robots have led to human casualties. Another question to ask is the ability of such machines to demonstrate ethical behaviour. This is, one of the greatest risks within the smart manufacturing framework and will need the careful attention of all stakeholders to mitigate. This requires rethinking in the way we design manufacturing tools and systems and the inclusion of ethical override algorithms into the computing core of such machines.

Risk parameter	Value
Time horizon	Now
Impact of threat	Medium
Difficulty to fix	Medium
To be fixed	Designers, regulators

3. Machines getting closer to how humans perform

Humans	Machines
Eye, ears, nose	Sensors
Arms	Robotic manipulators
Legs	Tracks, rollers, wheels
Brain	Computer core
Muscles	Hydraulics, electricals
Replication	73 per cent



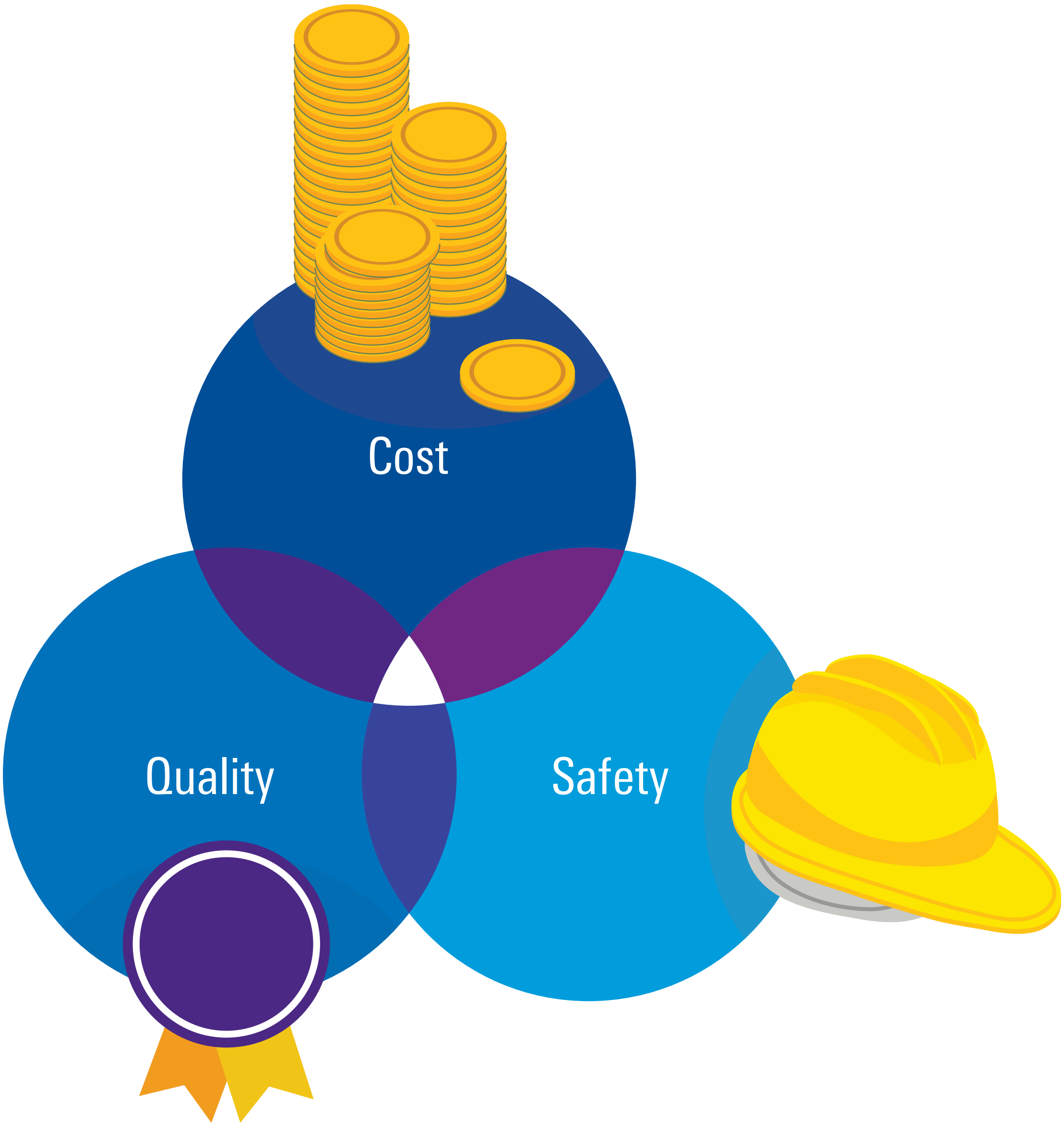
[02] First introduced in his 1942 short story 'Runaround'

[03] RepRap Snappy 3-D Printer (http://reprap.org/) accessed as on 17 July, 2016.

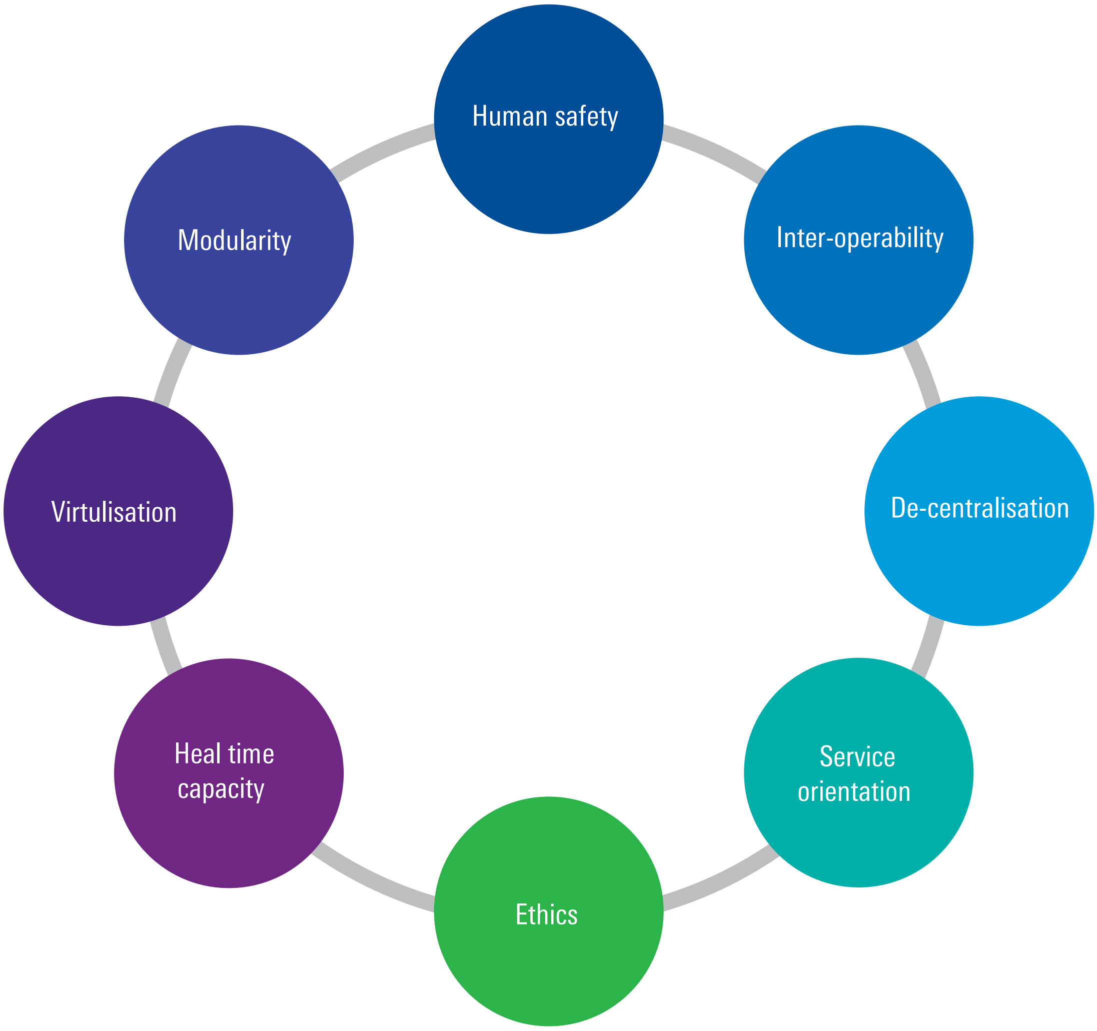
The change in design principles

The earlier design principles of manufacturing tools revolved around parameters that have an implication on the method of production and the end product (Figure 4). These frequently were parameters that reduced the cost of production, improved the quality of the end product and ensured that it was safe to produce.

4. Traditional manufacturing design principles



5. New design principles for smart manufacturing - emphasis on safety and ethics



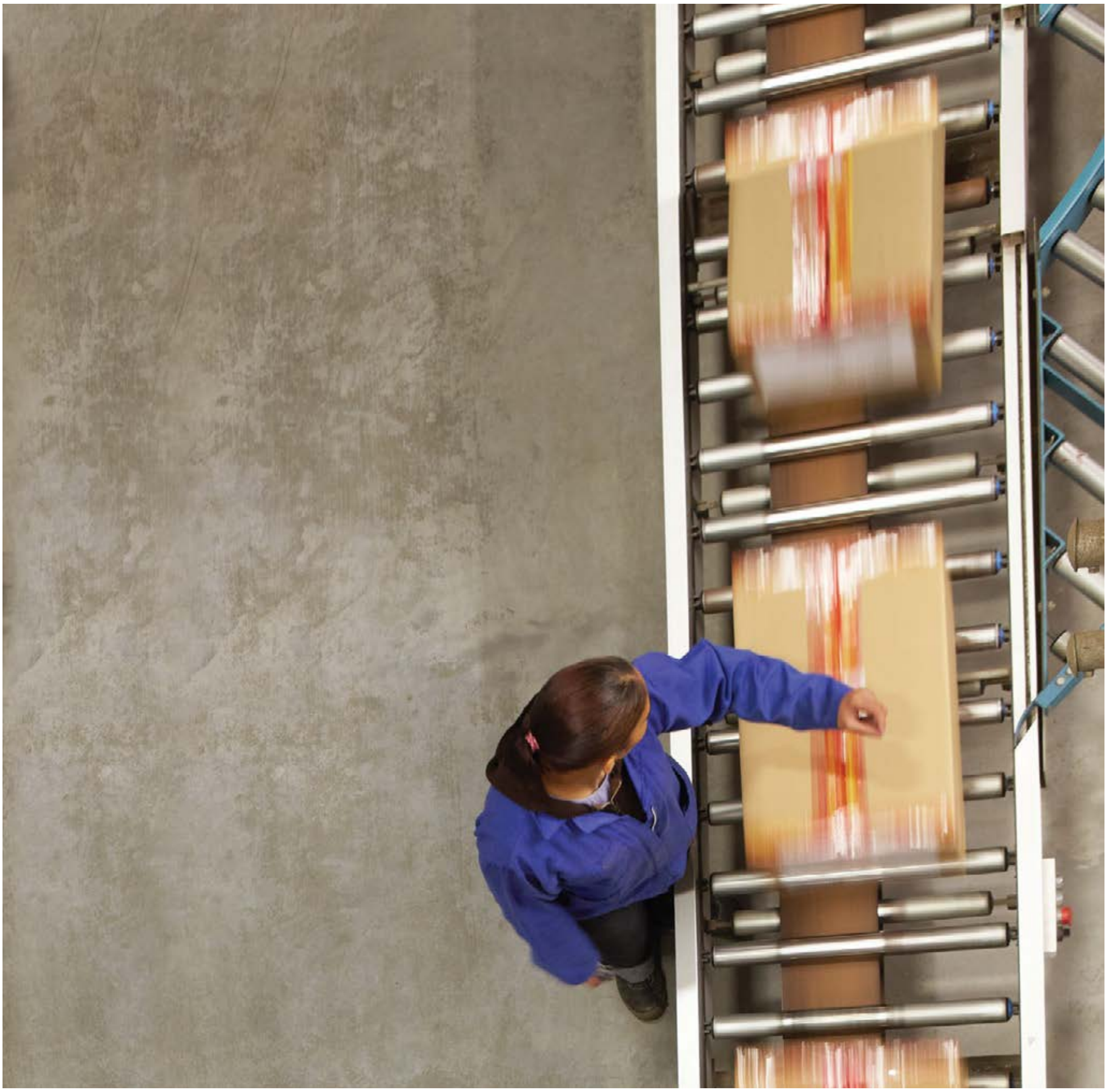
Mirroring the increased relevance of information technology in smart manufacturing processes, the new design principles that need to be used very closely resemble those followed while putting together large IT systems (Figure 5). While many of these are currently being followed, there cannot be a greater emphasis laid on the importance of both safety and ethics while designing systems within the Industrial IoT and smart manufacturing framework.

In fact, even within the information systems design for smart manufacturing, the traditional Confidentiality, Integrity and Availability (CIA) paradigm needs to shift to Confidentiality, Integrity, Availability, Safety and Ethics (CIASE). Designers need to ensure that any device that gets on the smart manufacturing set-up is configured to follow inviolate rules around safety and ethics. One approach that could be followed is for systems to be 'interrogated' prior to being allowed to join the network. Suspect devices and machines in this regime would be quarantined and allowed to join the network only on confirmation of their adherence to the safety principles that have been set-up. Based on the machine learning progress, some of the interrogation can be done by other trusted machines themselves, forming an almost self-governing federation.

> Designers need to ensure that any device that gets on the smart manufacturing set-up is configured to follow inviolate rules around safety and ethics.

Conclusion

All is not gloom and doom, however. In balance, for now, the benefits posed by the smart manufacturing framework far exceed the risks that they expose society to. Indeed for the information security segment of smart manufacturing, the recentness of this phenomenon is an advantage of sorts. Developers are able to address these risks as the solutions are being built. This is a lesson learnt after years of tacking on IT security solutions after the system has entered the market. The more difficult risks to address include the societal and human risks posed by the new technology. This requires careful analysis by thinkers from various disciplines including engineers, psychologists, economists and behavioural scientists to allow for appropriate risk mitigation strategies to be put in place.



Using technology to decode corporate fraud

Sandeep Gupta

Partner
Forensic Services
KPMG in india

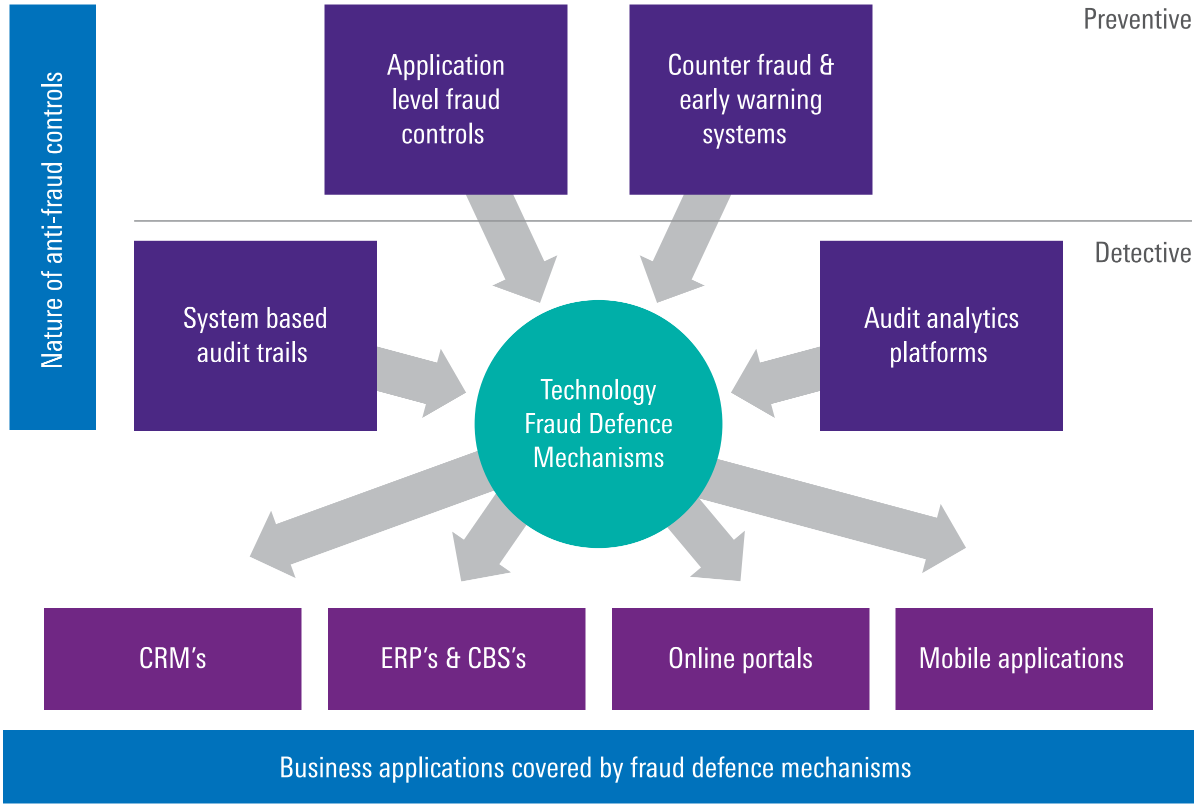
Challenges in this age of automation

Technology has taken a front seat in many businesses by serving as the backbone for communications, record keeping and automating business processes. With increasing technology innovation and constantly evolving business operations, companies are facing a new scourge namely 'technology-based frauds'. As business processes and transactions are increasingly being enabled by technology, the twenty-first century fraudsters leverage technology to execute fraud and cover their tracks. With the increasing complexity of IT applications used for business operations, traditional internal control mechanisms and internal audit sampling methodologies are being rendered less effective in the detection of fraud.

One of the greatest challenges organisations face in this age of digitisation and automation in fraud detection is to identify the pattern of frauds in the vast oceans of structured transactional data and their supporting unstructured data. In this light, it becomes vital for organisations to devise methods and controls to tackle the fraud risk challenges posed by data volumes.

Tackling the challenges posed by data volumes

In order to have effective internal control mechanisms to detect/prevent fraud in the current automated environments, it is imperative for organisations to inject data analytics into the operational processes and controls of the organisation, thereby making themselves more alert and resilient to frauds. Organisations have begun to implement a multitude of measures to decode the corporate fraud from the oceans of data. A snapshot of some of the measures that can be taken to facilitate effective detection of corporate fraud are outlined as under:


Nature of anti-fraud controls

Preventive

Application level fraud controls

Counter fraud & early warning systems

Detective

System based audit trails

Audit analytics platforms

Technology Fraud Defence Mechanisms

CRM's

ERP's & CBS's

Online portals

Mobile applications

Business applications covered by fraud defence mechanisms

Enabling audit trails

The key fail point in effective fraud detection and correction in many cases is the absence of audit trails. Organisations fail to identify those critical events/activities in ERP systems, SCM applications and mail servers that need to have logs/activity. Event logs from various servers have significant evidentiary value in determining the timeline for the activities leading up to the fraud and to a large extent in identifying the role of potential suspects in the fraud. An example of how audit trails/logs can help crack/decode clues in the corporate investigation is outlined as under:

Sr. no.	Fraud risk scenario	Evidentiary significance of audit trails (illustrative)
1	Fraudulent approvals in employee expense claim systems	Audit trail for log in events (with an IP address) - to obtain evidence to aspects such as: • Whether the account was logged into from any non-regular IPs, indicating compromise of credentials of the approver • Whether the account was logged into from any internal IPs, other than that of the approver, which could indicate compromise of the approver's accounts by an insider
2	E-mails imitating CXOs, sent to the finance department for transferring money to a fraudsters account	• Webmail user authentication logs – to obtain evidence if: - CXO account was logged into from any non-regular IPs, indicating compromise of e-mail accounts - Whether the account was logged into from any internal IPs other than that of the approver, which could indicate compromise of the approver's accounts by an insider • E-mail message logs – to obtain a timeline sequence of the communications surrounding the fraud and also if any additional suspects are involved in the fraud
3	Mass unauthorised changes to the price list on the sales module on the ERP, causing loss to the organisation	• User activity logs on the sales module – to detect the number of users active on the ERP and IP address from which they logged in to detect if the fraud was done internally or from outside the organisation • ERP table logs – to detect user IDs that made changes to price list tables and timing of the changes

Embedded fraud control in business applications

As the adage goes, 'prevention is better than cure', is an effective way of tackling frauds by embedding/configuring anti-fraud mechanisms within the business applications of an enterprise. The applications that require such anti-fraud controls range from CRM, ERP, payment portals, e-commerce portals and mobile applications used for business/payment transactions. An example of how controls can be embedded/configured in the ERP systems from a prevention perspective is outlined below:

Sr. no.	Fraud risk scenario	Anti-fraud controls embedded at an application level
1	Vendor payments to fraudulent bank accounts	• Bank field in the vendor masters in the ERP should be locked and allowed to be changed by an authorised personnel only and should be locked for other users • ERP to be configured to trigger an approval work flow for all changes to bank details in the vendor master • No changes to be allowed to vendor bank accounts during automatic payment runs • Segregation of rights allocated to users for conflicting duties
2	Duplicate payments	• Duplicate invoice check indicators to be enabled in vendor masters (this option is available in certain ERPs) • Configure a special customisation to determine if a particular amount has been paid to the vendor earlier
3	Fraudulent procurements	• ERP is configured with workflow based on delegation of authority document for approval of all Purchase Orders (POss) and invoices • Unused POs are locked • Tolerance limits set for over delivery of goods • Inability to process goods inward without a valid PO reference • Inability to enter invoices without valid goods inward and a PO reference

Counter fraud systems and early warning systems

A new range of systems that are slated to strengthen the battle against corporate frauds are counter fraud systems. These are designed to detect frauds from transactional data. The nature of counter fraud systems to be implemented vary from industry to industry depending on the level of fraud risk perceived and the value at stake. Organisations having large volumes/high value of transactions are now going for transaction fraud detection systems to ensure early fraud detection and remediation. Typically such systems have various components:

Data ingestion engines

This component of counter fraud systems generally ingests all transactional data that needs to be analysed for detecting fraudulent patterns. The ingestion engines in many counter fraud systems these days also have the abilities to ingest unstructured data namely news from the internet, social media, documents, scanned images and data dumps from non-standard applications.

Rule engines

This component contains the fraud detection logics that need to be applied on the transaction data to detect fraud. The rules that are configurable on the rule engines are of various types. A generic overview of various rules is as under:

Threshold-based fraud rules

These refer to traffic signal rules that are clear criteria-based, e.g. transactions that have been approved by persons beyond permissible limits, transactions without approvals, etc.

Pattern detection fraud rules

These rules are typically used for complex frauds, for example, in case of the banking environment, money trail analysis to detect fund trailing/tracing amongst certain sets of individuals. The output from these rules is typically in visual forms, indicating the flow of transactions across various accounts.

Predictive fraud rules

These are rules based on statistical models (for example, the Z model) that help systems bring out potential frauds based on the transacting patterns noted from the past. The systems are built with cognitive behaviour to help understand and evolve the rules to bring out more accurate results.

Alert engine

This component is generally responsible for comparing the ingested data with the rules mentioned in the rule engine to churn out fraud alerts. The rule engine has a detailed rating mechanism that helps rate the severity of the alert, so that both fraud analysts and investigators look at critical alerts on priority; alerts that are false positives can be marked as such. The alert engines also have machine learning capabilities to auto detect false positives based on past classification of alerts.

Case management and MIS

This model helps fraud analysts to pick relevant alerts and convert them into a case that can be accessible to the investigation team members and will have templates for documentation, evidence management, work flows for report review and approvals from the stakeholders.

Counter fraud systems in the banking and financial services sector

The banking sector is increasingly seeing value in implementing enterprise-level counter fraud systems. These systems are increasingly helping banks investigate a large amount of frauds/red flags. A brief example of some of the alerts/detection capabilities of the said system are:

Sr. no.	Area of operations	Anti-fraud alerting capabilities by counter fraud systems (Illustrative)
1	Corporate lending (fund-based	• Overall facilities (fund and non-fund) to a corporate or a corporate group level exceed the threshold approved exposure for the corporate/group • Limits for Cash Credit (CC) and Overdraft (OD) enhanced without proper Delegation Of Power (DOP) • Limits for CC and OD enhanced without approvals • Fresh OD facilities granted to Special Mention Accounts (SMA) /Non-Performing Assets (NPA) accounts
2	Trade finance	• Trade advances to customers for importing goods from smaller parties (e.g. individuals/proprietary concerns) in high-risk geographies/countries • Trade advances to customers for importing high-value goods (gold, diamonds) from smaller parties (e.g. individuals/proprietary concerns) based in high-risk geographies/countries.
3	Corporate lending (fund-based)	• Fixed Deposits (FDs) supporting live/active bank guarantees are refunded • Bank guarantees exceed the approved limit for guarantees • High value Letter of Credit (LC) issued to parties that have poor debt service/credit history.

Audit analytics

While the above systems are designed to work with the management on a proactive basis with a view to prevent or detect fraud in a timely manner, enhancing the internal audit department's capability to test fraud controls effectively becomes equally critical. Internal audit departments need to be equipped with audit analytics platforms to carry out red flag analytics as primer to their audit procedures and sample selection for document testing. Audit analytics tools come with a host of features that help the auditor to pick up the right samples for testing and provide insightful red flag reports. Some of the features of the audit analytics platforms are:

- Benford analysis for detecting anomalous transactions
- Statistical parameters for outlier detections
- Duplicate transaction detection
- Document sequence checking scripts
- Fuzzy logic testing on narrations/transaction descriptions/vendor to detect duplicate vendors/ fraudulent transactions
- Audit analytics platforms also come up with standard analytics script libraries for certain ERP systems to ensure that leading practices in fraud detection are leveraged by their audit teams. These analytics script libraries can be run automatically on standard data sets extracted from ERPs, which significantly reduces audit testing.

Building a road map for leveraging technology-based fraud detection mechanisms

In the present day and age, conceptually technology-based fraud monitoring solutions are the way forward for organisations. This being said, the success to deploy the above-mentioned mechanisms depends largely on the following key factors:

- Crystallising the needs of the business in terms of fraud risk monitoring
- Management commitment to the cause of fraud risk monitoring
- Dedicated team for implementation
- Alignment of the fraud detection systems to the business requirement
- Rigorous testing of the systems
- Sustainable monitoring model with dedicated resources for monitoring (based on the value at risk).

While technology is expected to play a great role in fraud detection, the continuing effectiveness of technology-based fraud detection systems largely depends on fraud risk intelligence configured on the detection systems. The higher the false positive alerts generated by the tool, the lower the reliance on the outcome. In conclusion, technology plays a great role to enhance the detection capabilities; however, the value from technology-based detection systems can only be derived if the right kind of people are used to configure the systems and drive the initiative to fruition.

Robotics/ cognitive technologies

Kalpana B
Partner
Management Consulting
KPMG in india

Introduction

An innovation that creates a new market and eventually disrupts the existing market, can be viewed as disruptive innovation. At the heart of disruptive innovation resides an upcoming practice of Robotics and Cognitive Automation (RCA). Automation essentially entails software or tools that create a platform over the existing business processes to perform day-to-day operations by reducing human efforts. RCA solutions focus on automating many of the mundane business processes such as invoice processing, standard reporting and month-end close activities that are high volume, repetitive and rule-based. The concept of RCA goes beyond automating only the manual repetitive tasks and provides an opportunity to automate decision support and factor in multiple variables to help make logically sound decisions.

RCA can be divided into three classes: basic, enhanced and cognitive automation. Basic automation covers automation of transactional, rule-based and structured data. Enhanced automation incorporates advanced technologies to enable the use of structured and unstructured data to support elements of self-learning. Cognitive automation uses advanced algorithms to allow automation of processes that are more perceptive in nature. Cognitive solutions incorporate advanced self-learning capabilities and can be used for sophisticated hypothesis generation or for advanced predictive analytics.

For RCA as a solution to become commercially viable, the process needs to be stable with high volumes of transactions. Only when the activity is repetitive and frequent, can the bots be profitably deployed. Some other traits that should be verified are use of structured data, rule-based decision-making, standardised and stable processes. These process traits indicate that automation can yield faster deployment and quicker returns – a good fit for basic automation.

Intelligent automation such as the enhanced and cognitive automation can be deployed once basic automation is leveraged. Intelligent automation, coupled with basic automation, has a potential high degree of impact on the business top line.

The applicability of RCA may include automating processes by mimicking repetitive human actions through knowledge augmentation with enhanced decision-making of skilled professionals such as executives, accountants, attorneys and scientists. Finance and accounting, procurement, IT, HR and payroll management are a few typical areas where the transactional processes are being automated. RCA is predominantly applicable but not limited to high volume, labour intensive, involving structured data, repetitive and rule-based processes. Advanced forms of RCA can be used to automate complex decision-making, business critical processes and processes involving unstructured data.

Robotics in the Indian context

In the current ecosystem, the fraternity of shared services centres and global in-house centres (GICs) around the globe and India are prime clients for RCA solutions. Client organisations are modifying their vision strategy to encompass RCA as part of the business strategy. Clients are reconsidering their sourcing choices and are exploring automation vendor capabilities to meet requirements. Existing outsourcing contracts are being considered for revision with automation services. GICs are assessing and developing in-house capabilities to adopt RCA by setting up automation centres of excellence (COE) to drive organisation-wide projects. Dedicated organograms for automation COEs have evolved within these organisations. Service providers have developed automation platforms that can be integrated with different automation tools in the market. These synergic partnerships are leveraging different capabilities, and are striving to make the offering robust and complete. These service providers are also implementing these solutions in-house to their business process outsourcing centres.

India, being one of the key sourcing destinations for global firms, is the base for large scale shared services set-up, and one of the largest markets for business process outsourcing. Businesses leverage labour arbitrage to create additional value, thus enabling them to focus on core business activities.

Businesses continue to face three broad set of risks due to a variety of reasons:

Operational risks due to slippages in quality, cost or speed of process execution

Strategic risks related to issues such as protection of intellectual property, security and privacy

Composite risks, which are long-term risks, such as losing the capability to execute business processes in-house due to loss of talent and knowledge of the business process.

India Inc. has already spent considerable amount of resources in identifying the critical risk components and creating frameworks to keep these risks in control. In the current market space, we see an increase in regulations and compliance-related activities that resulted in the creation of siloed approaches to individual process that adhere to these compliance requirements. This has resulted in the duplication of risk management efforts. Business leaders are struggling to see the value generated by these activities and view them as a cost of doing business rather than an investment to improve corporate performance.

Risk and robotics

In the risk management space, RCA can perform a predominant role in helping organisations comply with the regulatory requirements while also addressing the control requirements. Robots comply with processes and strictly adhere to the codes. Hence, operational risk involved in accounting procedures, data management and even reporting are considerably reduced. Robots interact with finance and business tools, manage service requests automatically and, at the same time, complete the entire accounting close process and provide accurate results.

Reconciliation processes are currently one of the most manual-intensive aspects where the scope of risk is very high. RCA enables swift and clear reconciliation processes to identify clear mismatches and escalates to the right point of contact. RCA can enable the identification of potential areas of high risk exposure and also analyse the cause for potential risk areas.

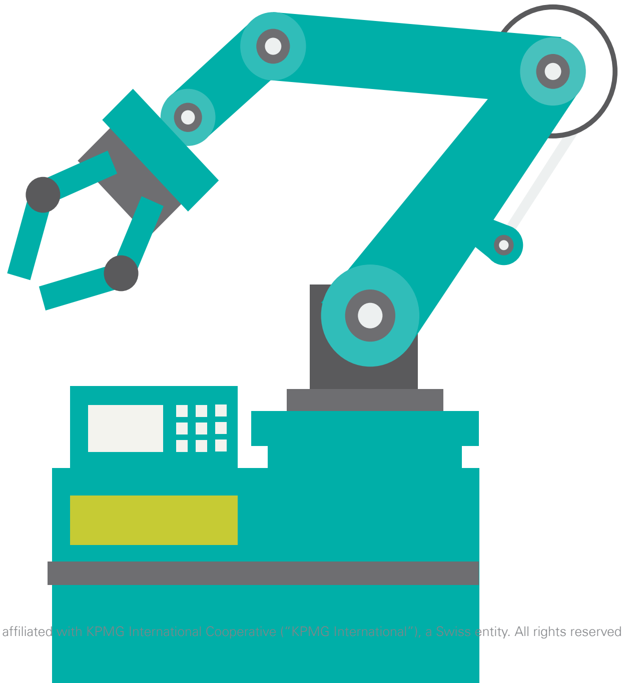
Robotics and cognitive technologies support organisations in automating processes and reduce human touch points. Manual operations pose one of the key risk areas for organisations. Even with a lot of process controls, organisations find themselves susceptible to either incorrect operations performed or the incorrect inference of the data. Due to the large volumes of back-end operations, companies tend to lose track of these small errors, which accumulate over time. RCA can help mitigate these risks by eliminating a majority of the manual process activities and creating a transparent view of process operations. RCA can help reduce the false comfort, unreliable information, costly and inefficient execution of multiple compliance activities and the lack of transparency due to manual adjustments. RCA also brings in control mechanisms not just in financial activities, but also in business activities.

Automation tools can be used for efficiency through basic automation by doing more things in lesser time, or for effectiveness, where you move into a cognitive engine of automation. RCA tools are different and the typical features of these tools include scalability, governance, compliance and minimum intrusion to the existing IT landscape. Standard automation tools come with a control tower feature that provides a centralised monitoring solution to govern all the automated processes using robots (also known as bots) running in the production environment. RCA tools maintain extensive logs/trails that support auditing of the automated processes. Since most processes are governed by certain rules, clear-cut exception to the processes are easily highlighted when the robots are running. These exceptions can be either handled outside the robot by manually intervening in the process or the cognitive robots can be programmed to handle these exceptions. As you see human intervention getting minimised in processes, it brings better controls, which ensures that most process risks are mitigated.

The standard risk and compliance framework involves several activities, which include defining the risk profiles based on assessment of the organisation, building control frameworks within processes, compliance and performance reporting, assurance reporting, building risk and a compliance-based culture. Some of these key activities are addressed using technologies that automate the processes.

RCA can play a key role in the banking and financial sector, which currently employ a large amount of resources in India. Financial processes can be automated bringing in a large amount of control to the processes. Regulatory reporting requirements can be scheduled on the robots, and can provide a faster turnaround time on these processes.

Financial processes in the shared services centres are almost the same with some amount of variation based on the company/clients. The Know Your Customer (KYC), Anit-Money Laundering (AML) or the Fair and Accurate Credit Transactions Act (FACTA) regulations impose an overwhelming number of requirements that banks and financial institutions must meet before they do business or continue doing business with customers. RCA as a solution takes care of these requirements and reduces the risks like absence of audit trails, data theft, use of wrong data, manual errors, etc. RCA provides timely, accurate and faster output, which helps in reducing reputational damage because of non-adherence of commitments to vendors, employees, banks or government authorities.



Conclusion

Robotics and cognitive technologies not only support in managing the risks for an organisation, but can help eliminate potential operational risks. The new-age disruptive technologies bring much needed controls within an organisation. Organisations should not overlook some of the risks that are associated with the implementation of RCA. The importance of IT security increases drastically with the use of RCA technology. Malicious codes, if added to the robot engine, can create backdoors or even send internal confidential information outside the organisation. The user might not even realise when these documents are being transferred since most of the robots run in the back-end of the IT systems. It becomes imperative to review and assess these programmes by performing code audits periodically.

Automation specific business continuity plans would be the emerging standard along with the era of robots. Automation platforms, just like other IT systems, are prone to failure risks and therefore should be secured with robust BCP guidelines within organisations.

The new age organisations have recognised robotics as the next stage of evolution for their business processes. In addition to the benefits of cost and quality, robotics bring in process transparency and better controls that help in mitigating whole basket of risks that organisations currently face.

The risk landscape within organisations is changing dramatically. As existing technologies are increasingly being disrupted, we see a dramatic role of robotics in supporting organisations and mitigating the risks of disruption. Day-by-day new types of business and finance process risks are being identified. Robotics enables organisations to reduce their effort on control areas and concentrate on driving businesses.

Conclusion

The world of technological advances is a double-edged sword, where one needs to embrace technology along with its strategies, as well as simultaneously mitigate the associated risks. Abstinence from any of these technologies might appear as one of the most effective defenses, since ensuring compliance is an uphill task. But the exponential rate at which the digital world is booming, it is likely to influence organisations in the years to come. The various chapters in the report highlight the potential of adopting stronger policies, implementing stricter controls, increasing employee awareness and taking the necessary actions to mitigate risk.

The more we move towards innovation, the more we expose ourselves to the dynamics of risks. However, with the evolution of technology, new security features and proficiencies are likely to emerge. Organisations need to build and implement leading practices for effective risk management.

We believe that a dynamic India Inc. will emerge by being resilient in the face of a global turmoil, while facing the challenges on its expedition to success. During this journey, several questions need to be answered:

Will the challenges in the regulatory environment bring in the desired level of change? How do we insulate ourselves despite the volatile global business and political environment? What needs to be done to ride the cognitive and robotics technology wave, and use such technologies to grow better, faster and stronger? Can the financial services sector manage the demands of regulators, and stay current and upbeat with the emerging trends? Will India Inc. counter the threats posed by cyberattacks to build stronger technology defense mechanisms? Will we be able to build adequate early warning systems to manage the probable corporate frauds, global financial uncertainties and any crisis that comes our way?

Our publication 'De-risking India in the new age of technology' looks at several challenges that India Inc. may encounter in the near future. We have also proposed different ways in which the risks arising out of the business environment can be suitably managed.

We hope our analysis assists you in answering a wide array of questions to manage the risks with poise.

Acknowledgements

We acknowledge the efforts put in by the following team members:

- Ashita Parekh
- Angad Singh
- Aamir Munshi
- Arjun Chandra
- Bonny Desai
- Disha Agarwal
- Deepak Viegas
- Eswar Subramanian
- Hemang Jauhari
- Jignesh Oza
- Mayuran Palanisamy
- Pritam Magar
- Dr Pinaki Ghosh
- Prashant Bhat
- Priyanka Agarwal
- Rohit Krishnan
- Rebekah Paul
- Reshma Pai
- Rami Reddy
- Rohit Nair
- Rukmani Vishwanath
- Suangna Singh
- Sameer Hattangadi
- Sheekha Panwala
- Shatadal Ghosh
- Sriram Chakravarthy
- Shreya Khanna
- Shailesh Indapurkar
- Vidya Mohan
- Vivek Kedia

KPMG in India contacts:

Nitin Atroley
Partner and Head
Sales and Markets
T: +91 124 307 4887
E: nitinatroley@kpmg.com

Mritunjay Kapur
Partner and Head
Risk Consulting
T: +91 124 307 4797
E: mritunjay@kpmg.com

KPMG.com/in

The Confederation of Indian Industry (CII) contacts:

Greeta Varughese
Executive Director
CII
T: +91 80 4204 4097/98
E: greeta_varughese@cii.in

cii.in

Follow us on:
kpmg.com/in/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

This document is meant for e-communications only. (021_THL0816)