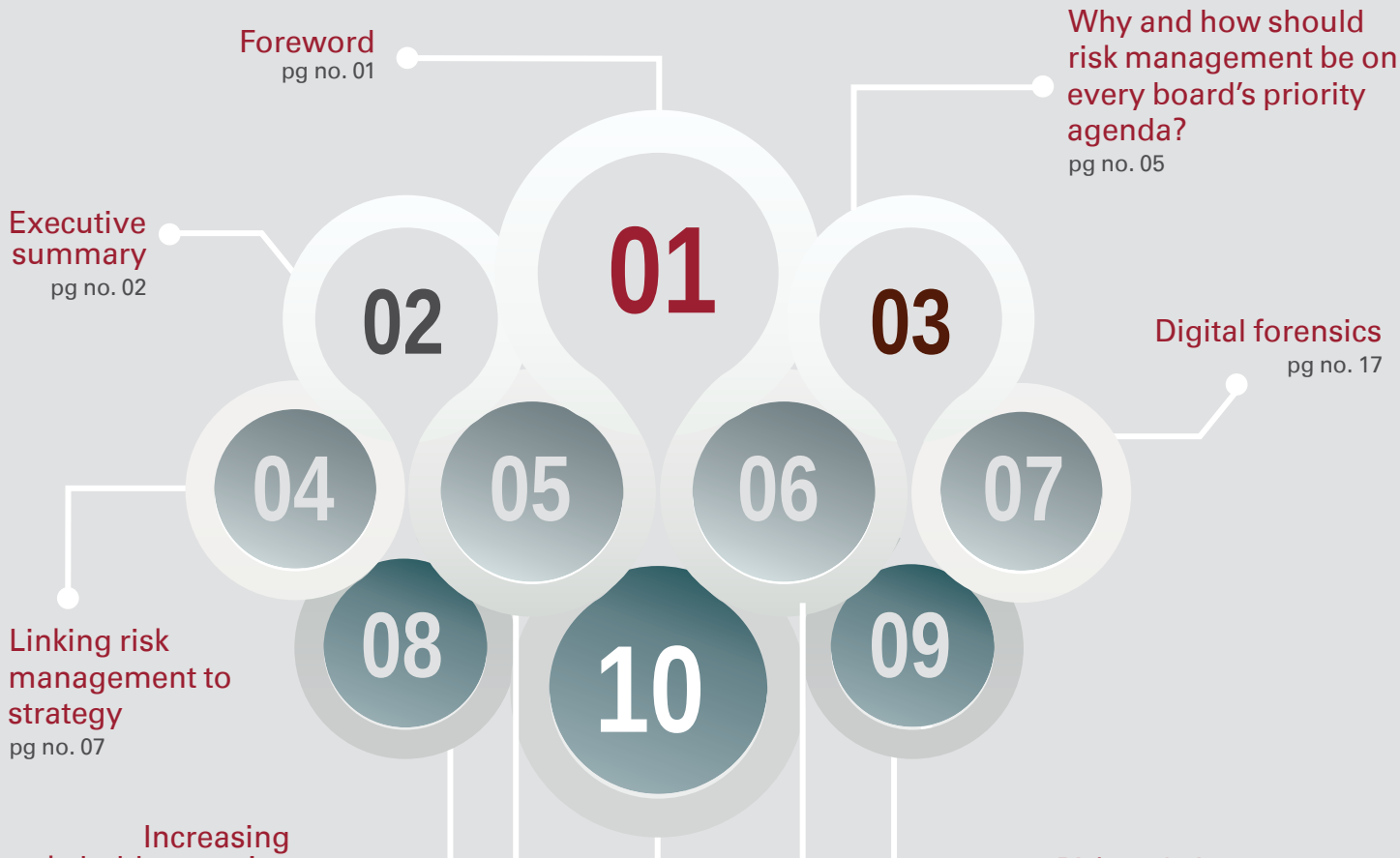
KPMG
cutting through complexity

CII
Confederation of Indian Industry

Derisking the future of India Inc.

kpmg.com/in
cii.in

Table of contents



Foreword

The Indian economy, riding the wave of populist sentiment in electing a majority government, is poised to take major strides forward. Infrastructure, foreign investment, and fiscal prudence are some of the key factors expected to hold sway in India's march towards establishing a global economic powerhouse.

For every GDP driver that the government is looking to improve there are Risks strewn across the business landscape. In India's quest to move up the value chain viz-a-viz innovation we are glossing over the challenges arising out of storing, managing, and guarding data, the rampart of our thrust towards economic premiership in a globalized, interconnected word. WE are carrying forth the flag of "Made in India" but In this race to be the sought after providers of services and products, we may be guilty of being lax when it comes to understanding, evaluating holistically, or, in worst cases, even considering the risks that operations face in these complex times. Risks, such as those arising from 'Frauds', 'Loss Of Customer Data', 'Privacy', 'Climate Change', are but a few of the ever present threats to organizations' short and long term operations, and potentially capable of destabilizing business continuity.

As the generation that started working in the private sector during the onset of liberalization, we were privileged to watch and contribute to the growth of the businesses and firms that chose to dream big and consequently, as a collective, helped the Indian economy take strides towards playing catch up with the rest of the world. Those were the heady days of seizing opportunities, understanding global players, developing in-house capabilities from scratch, and overcoming challenges as we began new and more efficient economic participation. But what we saw during those days pales in comparison to the changes and disruptions that the economy, as part of the global network, has witnessed over the past decade or so. A veritable cornucopia of supply/ demand dynamics, concomitant technologies, and deep interdependencies, among and within economies, has led to business growth, disruption, and closures at a magnitude hitherto not imagined or seen.

The explosive growth in communications and transportation technology coupled with the opening of new economies and positive investor sentiments has been among the key drivers of the rapidly changing and often volatile global business landscape, and has had ripple effects across the entire value chains of businesses. The old guard, such as 'Financial Management' and 'Capacity planning', of business management is now merging forces with the young upstarts, such as 'Data Analytics' and 'Social Media', in the race to meet, drive, and channel consumer demand, a capricious beast at the best of times, across price points and utility functions at a scope and scale yet unseen.

Risk management, by its very definition, requires a deep rooted commitment to safeguarding stakeholder interests through protecting customer data, ensuring regulatory compliance, sustaining the environment, or even preserving shareholder value, amongst others.

The ramifications of an absent risk management initiative can be best illustrated by the events in Japan. No one could have predicted the earthquake in Japan but an appropriate risk management framework would have considered the likelihood of such an event, the loss of components arising out of one, and made obvious the benefits of diversifying suppliers; a plan that, if implemented, would have mitigated to some extent the business losses arising out of the earthquake.

Risk exposures, though omnipresent and multifaceted, can be managed through proper planning, including risk identification, and implementation based on the foundation of understanding the dynamics of the business, customer, and society, as a whole. Another point that begs mention is the setting up of Early Warning Systems as risk threat indicators, the absence of such indicators leaving organizations cruelly exposed to dynamic, quick, and massive negative events, sort of an avalanche in the Andes.

This conference aims to discuss the need for defining, analyzing, understanding, and mitigating risks in the context of business operations, customer needs, and societal responsibilities in an intricate economic environment. On behalf of CII and KPMG, we would like to sincerely thank the sponsors, industry experts who have graciously agreed to contribute their time and knowledge to this endeavor. We are confident that their efforts will prove instrumental in raising awareness and engaging various stakeholders on the key need of the hour – Risk Management.

Suresh Senapaty
Chairman, CII National Risk Summit 2015
& Executive Director and Chief Financial Officer, Wipro Limited

Mritunjay Kapur
Head, Risk Consulting
KPMG in India

Executive summary

After subdued growth in the past few years, driven by global and domestic factors, India's economy now seems to be out of the woods. Potentially game-changing developments over the past few months gives reason to believe that the Indian economy may well be at an inflection point. 'Make in India': an initiative of the new political establishment to revive manufacturing is one such development which aims to provide the much needed impetus to India's long-term economic recovery. Undoubtedly, the sentiment seems to have shifted from 'risk off' to 'risk on'.

This change in sentiment from both domestic and global investors' point of view can augur well for the overall business environment in India. Enterprises, however, need to be guarded in their approach as deepening integration between economies world-wide has only added to the complexities. Occurrence of a risk event in one geography can impact the other regions within no time with very limited response time. Take the case of 2011 earthquake in Japan. Consequent to the earthquake, many automobile manufacturers had to suspend operations at some of their manufacturing plants due to disruption in supply of parts from Japan. Similarly, other industries such as consumer electronics and electronic equipments were also impacted as Japan is a key supplier of parts to these industries globally[1]. Such risk events can have a ripple effect on companies that have been exposed to the affected countries/regions. It is a glaring instance of how even an unconventional factor may have severe repercussions on enterprises.

The risk landscape has indeed undergone a vast change over the past few years. The degree of uncertainty is only likely to increase for enterprises as their involvement with global supply chains increases due to the sheer number of variables and their complex inter-dependencies. In addition, the speed and the magnitude with which these risk events occur can potentially de-stabilise the long-term sustainability of an enterprise. It is thus imperative for concerned stakeholders to exercise greater caution and look for ways to mitigate these risks.

It is no surprise then that regulators world-wide have also realised the importance of corporate risk management and have been tightening their grip in order to protect the interests of various stakeholders. For instance, the Committee of Sponsoring Organisations of the Treadway Commission (COSO) updated its internal control framework in 2013 considering the changes in business and operating environment. In India, the enactment of the Companies Act, 2013 and SEBI's revised Clause 49 guidelines of the Listing Agreement are also a case in point. Regulations are also evolving in areas such cybersecurity and climate change. As a result, such fast paced evolving regulatory environment is placing onerous responsibilities on executives to review and strengthen their corporate risk management capabilities. An inability to do so is likely to have far-reaching implications not only in terms of higher costs of compliance, but may also result in significant losses and damage to corporate reputation.

1. 'Japan supply chain break down to hurt global production', BBC News, 25 March 2011

Akhilesh Tuteja
Head, IT Advisory
KPMG in India

Contemporary risk themes in a dynamic business environment

Given, the fast-paced nature of the business environment, we believe the following risks have become even more relevant than ever before.

Growing importance of financial risk management in a volatile world

The sharp rise in the volatility in global financial markets and the sophistication of financial instruments have continued to impact the earnings and profitability of enterprises (especially the ones with unstructured financial risk management systems). For instance, Euro has depreciated sharply by about 7 per cent against the Indian rupee (INR) from 82.1084 on 2 July 2014 to about 76.3276 on 10 November 2014[2]. Such volatility can have a significant impact on Indian companies exposed to the Eurozone considering that it is India's second largest partner for external trade[3].

Growing menace of frauds, IPR and counterfeiting

Intellectual property (IP) and counterfeiting related frauds are widespread in India. Companies have been suffering significant losses in terms of revenue leakages. While difficult to quantify the extent of losses, according to The Confederation of Indian Industry (CII), the FMCG sector loses about 15 per cent of its revenues to counterfeit goods, with some brands losing as much as 30 per cent of their business to IP related crime[4].

Emergence of cybersecurity and data privacy risks in a digitally enabled enterprise

Extensive use of technology in this hyper-connected world has meant that enterprises are increasingly becoming vulnerable to the risk of cybercrimes. According to a recent study by Ponemon Institute, it costs U.S. organisations an average of USD12.7 million to detect, recover, investigate and manage incident response post the attack[5]. Cybersecurity is thus fast emerging a major area of concern as the intensity of cyber-attacks continue to grow. To mitigate the risks of cybercrime, companies have to continuously invest in safeguarding their technology infrastructure to thwart any potential cyber incident.

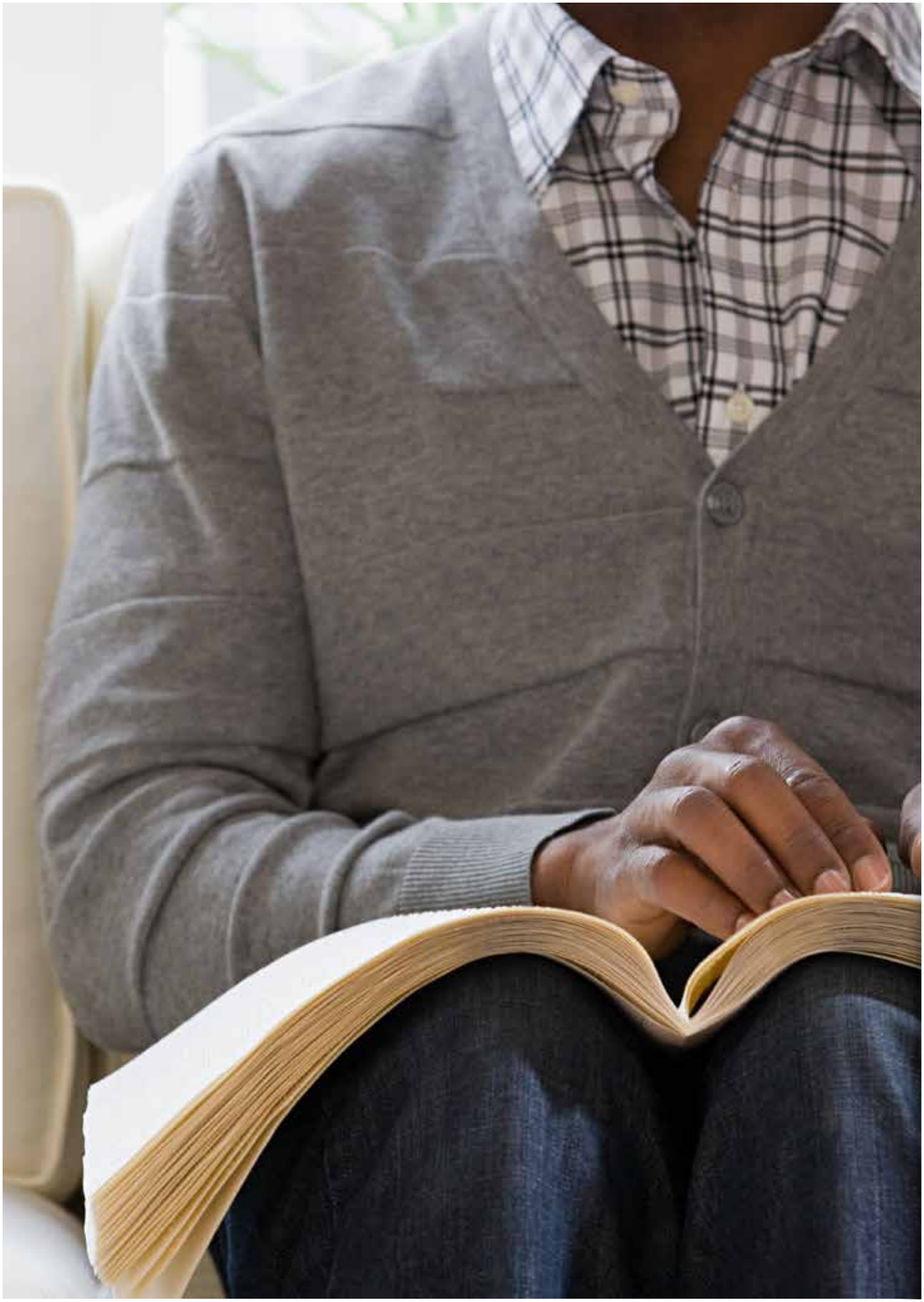
Increasing stakeholder scrutiny in reference to climate change and sustainability related risks

Even as enterprises realise the importance of climate change and sustainability related risks to their businesses, anecdotally it appears that companies are largely unprepared to manage such risks. Many Stakeholders, especially regulators and investors, are keeping a close watch on the carbon footprint of the enterprises. Companies should now engage actively with the stakeholders in the supply chain to reduce the adverse impact of their operations and supply chain on the environment.

A formal and effective risk management framework can help the firm endure such uncertainties. By providing inputs to the business to make informed decisions, an effective risk management framework can act as a facilitator for exploring new strategic business opportunities. It can thus play a crucial role in helping an enterprise develop its competitive edge and maintain its long-term sustainability. But for this to happen, enterprises and stakeholders need to change the perspective towards risk management. There is a need to change the approach towards risk management.

An 'as is' analysis of an enterprise's current risk management practices could be the starting point. This would require an in-depth introspection with some pertinent questions. How far is risk management integrated into the company's strategy planning? How often do we articulate, assess and aggregate risks at an enterprise-wide level? How efficiently are we utilising our resources to manage risks across the enterprise? More importantly, how effectively are we developing and nurturing our risk culture at an enterprise-wide level? Do we have an understanding as to how the risks built-into our operations impact the company's financial results? The answers to these and more such questions will assist organisations in enhancing their risk management capabilities. To de-risk the future, it is crucial that companies develop a proactive risk management framework with a forward looking approach to managing risks. It should help in unlocking value by prudent risk taking.

2. Based on daily historical data extracted from www.oanda.com
3. 'How euro depreciation impacts Indian companies', Moneycontrol, 23 September 2014
4. 'India: IP CRIME: 'Rising Threats To Intellectual Property Rights", Mondaq, 17 June 2014
5. 'Average Cyber Crime Incident Costs Companies $12.7 Million', www.tripwire.com, 15 October 2014



Why and how should risk management be on every board's priority agenda?

As per NACD's Blue Ribbon Commission, boards need to be cognizant of the following kinds of risks that companies typically face (risks discussed in previous sections could be included under some of these categories)[1]:

- Governance risks: Risks emanating from the decisions of the leadership and the structure and composition of the board and management.
- Critical enterprise risks: These are five to ten high ranking risks that can threaten the very existence of a company, specifically its strategy, business model or viability.
- Business expansion risks: As the name suggests, these are risks emanating from a company's organic or inorganic growth. It could include risks from acquisitions, major investments, entry into a new market, etc.
- Business management risks: These risks include risks arising from day-to-day operations.
- Emerging risks and non-traditional risks: These are risks due to extraneous factors such as changes in technology, changes in customer demographics, climate change, etc.

With risks emanating from so many areas, it easy for companies to lose sight. This is where boards step in. They should help the company's management in broadening their horizon of risk sources, understanding risks and the interplay between them, and assist them in managing risks at a portfolio level than at individual risks levels. In order to do so, it might be helpful to firstly include 'risk management' as a prominent agenda item in board meeting agendas. In fact, recent regulatory requirements – that demand boards to evaluate and attest the company's risk management framework is effective – has made it necessary for the boards to do so.

At such meetings, discussions on risk management should focus, among other things, on: (a) underlying assumptions in strategic decisions, (b) risk appetite and tolerances, (c) extent to which these are incorporated into objectives, policies and procedures, (d) extent of aggregating and integrating risk exposures, and (e) effectiveness of mitigation strategies.

While the board has responsibility for risk oversight, standing committees should discuss risks emanating from their oversight areas and help the board build a larger picture of the risks the company is facing and management's ability to manage them. As per regulations, in many companies an audit committee has been given the mantle of risk oversight. In case of banks and top 100 companies by market capitalisation, SEBI and RBI require a separate risk management committee to be constituted. However, in both the cases other mandatory board committees such as 'nominations and remuneration' committee, CSR committee and stakeholder relations committee are not absolved from risk oversight responsibilities. They could assist the audit/risk committee by overseeing risks in their area and passing on relevant information in a timely manner. Especially in case of the audit committee, given its limitation (owing to oversight of crucial areas such as financial reporting, oversight of auditors, etc.), it may become necessary for the committee to restrict its role to that of an aggregator.

1. 'Risk Governance: Balancing Risk and Reward,' National Association of Corporate Directors, October 2009

In summary, some of the below mentioned principles could assist boards in strengthening their risk oversight and customising it to the specific needs of their companies.

Some principles to help avoid risk oversight

i. Understand the company's business model, industry and supply chain, along with its positives and challenges

ii. Identify risk oversight responsibilities at the board-level and explicitly state these responsibilities in board and committee charters

iii. Assist management in setting and periodically reviewing risk boundaries defined by risk appetite and tolerance levels

iv. Evaluate if these limits are integrated into the company's policies, procedures and controls

v. Discuss with the management risk categories, concentration and inter-relationships, including mechanisms to identify, assess and mitigate them

vi. Establish criteria, standards and processes for the management to report the company's risk exposures (especially risks that can make or break the company) to the board

vii. Review the company's compensation policy and its impact on the ability of employees to take prudent risks

viii. Constructively challenge the management on their risk assumptions, assessments and mitigation strategies

ix. Help ensure that there is alignment in the company's strategy, risks, regulatory compliance, assurance and controls.

Linking risk management to strategy

It is imperative to address risk management at a strategic level rather than at functional/business unit levels. Effective risk management that defines, characterises and measures the probable negative impacts of interconnected global risks can aid organisations reap several benefits in a globalised environment. How organisations manage these risks, can be a game changer for the future of India Inc.

Every crisis reminds managements and boards of a costly lesson that risks gone bad in one part of the economy can set off a sequence of events in quarters that may seem completely unrelated. Risk management is often seen as a tool for validation of internal controls and for complying with regulations like Listing Agreement (SEBI) and the Companies Act.

According to Professor Richard Foster from Yale University, the average lifespan of a company listed in the S&P 500 index of leading US companies has decreased by more than 50 years in the last century, from 67 years in the 1920s to just 15 years today[1]. Alternatively, take the case of some leading companies in the mobile handset space which were once considered to be the pioneers of their respective domain. A major reason many of these companies may have failed was due to their inability to keep pace with the technological advances and their respective competitive landscapes thereby threatening their survival. The complex business environment, advances in technologies and shortening product cycles have resulted in growing risks that organisations are facing. In addition, the tightening compliance requirements have only added to the complexities. Boards and managements are thus increasingly realising the importance of risk management in the long-term sustainability of the business.

However, not all companies have a structured approach to monitoring and managing these risks. A structured approach would help organisations to consider, among other things, unintended consequences of their decisions, multiplicities in regulatory compliance, interrelationships between various risks, emerging threats, etc. In case of organisations with multiple subsidiaries, consistent application of such an approach across subsidiaries becomes necessary.

While a company's management is responsible for establishing a structured approach, its board should guide the management in this endeavor by broadening the management's horizon of risk scenarios and mitigation strategies.

1. 'What Do Business Leaders Need to Unlearn?,' Digital Marketing, 12 May 2014

Adopting a structured approach

Boards should urge companies to adopt a holistic and structured approach to risk management in dealing with the evolving risk landscape and regulatory environment. The desired structure should break the silo-ed approach generally observed in many companies and should encourage sharing of information between different functions across the organisation with clear risk reporting responsibilities and escalation matrix. An enterprise-wide risk-aware culture needs to be instilled over a period of time that can place the organisation on a firm footing to mitigate various risks.

A structured approach would involve:

- **Facilitating effective Board and CxO oversight of risk management:** It is essential that board members collectively assume and share the full responsibility of risk oversight and embed it into the strategic decision making process. A CxO/CRO level executive should ideally lead the day-to-day risk management efforts with direct access to board members. Some of the key actions that may lead to this include:
  - Documenting acceptable levels of risk appetite and tolerance limits via a risk policy
  - Distributing risk responsibilities across the organisation (making it everyone's responsibility)
  - Establishing appropriate organisational structure and reporting lines
  - Communicating the strategic intent behind the policy, reporting lines and responsibilities to all employees.
- **Establishing formal risk management processes:** Board members should ensure that formal risk management processes are established to identify, analyse, evaluate, monitor and mitigate risks on a real-time basis. Some of the key initiatives that may help in operationalising this include:
  - Establishing processes and controls keeping in mind risk appetite and tolerance limits
  - Including risk management responsibilities as a part of job description and individual objectives
  - Identifying risk-based key performance indicators
  - Linking them to performance management
  - Identifying and implementing monitoring processes and methods of feedback (including assurance and whistleblower mechanisms).
- **Facilitating a risk aware culture:** Creating an enterprise-wide risk aware culture would require setting the right tone at the top by making risk management as an imperative agenda at the board level. This may also require providing periodical risk management training across the enterprise, assigning specific risks to the respective process owners and possibly even linking their performance management process over a period of time. Some of the key initiatives that can assist in promoting a risk aware culture include:
  - Using commonly accepted definitions of risk
  - Educating employees, at all levels, including board and senior management, on appropriate risk behavior
  - Rewarding right risk behavior
  - Embedding risk champions within business functions and subsidiaries
  - Leveraging information technology to share knowledge on risk management.

While the entire board would be responsible for effective oversight of risks, multiple committees of the board (either as mandated by local regulations or on need basis) may be set-up to provide oversight on specific risk areas, depending on their knowledge on the subject.

According to a report on global risks by the World Economic Forum, 'The growing trend for boards to be involved in risk management is creating opportunities to shift organisational cultures away from a focus on quarterly results or daily share-price movements and towards the kind of longer-term thinking that is a prerequisite for addressing global risks.'[2]

The aforementioned statement underscores the need for boards to get actively involved in the risk oversight functions on account of growing complexities in the overall business and risk environment. In doing so, board members may need to facilitate alignment of strategic objectives with its associated risk by understanding and challenging the assumption made by the executive management through 'what-if' scenarios. Board governance over risk can be enhanced through proactive involvement in evaluating the company's strategy.

In order to help ensure higher degree of involvement in strategy and appropriate evaluation of strategic risks, directors need to have access to the right information. They need to invest time in defining their information needs and conveying it to the management. Standardising board briefing packs and agreeing on key performance indicators that are to be tracked and reported is likely to help the board in this effort. In regards to KPIs, it makes sense to have both lead and lag indicators of not only financial performance, but also non-financial performance.

Additionally, board members would need to engage in regular dialogue about risks with various internal and external stakeholders to validate the management's risk assumptions. Given the regulatory reporting requirements thrust upon board members, they would have to play a pivotal role in facilitating setting up of a robust risk structure which can lead to a risk-aware culture of 'no surprises' and help ensure its link to strategic decision making.

2. World Economic Forum: Global Risks 2014 Ninth Edition

Growing importance of financial risk management in a volatile world

Ruchira Dabas
Partner, Finanacial Risk Management, KPMG in India

Introduction

'Market volatility' has become a buzz word in recent years where an unexpectedly high volatility was observed across asset classes: be it capital markets, currencies or commodities. Both financial and non-financial institutions were put to test on their ability to cope with the dynamically changing financial environment in which they operate, as long standing correlations broke down and stress testing scenarios became a harsh reality. The combination of economic frailties in the developed world, geopolitical uncertainties and weak macroeconomic positions on the domestic front led to a particularly difficult situation for the emerging market economies, including India. The erstwhile engines of global economic growth, 'BRICS' slowed down considerably and commodity prices as well as currencies saw huge swings threatening the world recovery and shaking many corporations to act in the area of financial risk management. Volatility and uncertainty in the markets has brought greater focus to risk management as a function which is now viewed more positively compared to pre-2008 crisis days where it was primarily a low priority support function.[1]

Foreign exchange risk: How to survive in a volatile FX market

Financial markets have been in turmoil over the past few years with currencies displaying high degree of volatility. INR has witnessed unprecedented depreciation against the USD driven by both global and domestic factors and it lost more than 20 per cent value over a period of few months (May-August 2013). [Chart 1] However, after timely measures by the Central Bank and political stability at the centre, it recouped a good part of its losses and has been relatively less volatile in 2014. The 'twin deficit' problem still persists and with high dependence on the FII flows, INR can not perhaps be relied upon as a stable currency.

Chart 1: USD INR currency movement

Source: Bloomberg

Further, foreign currency borrowings by Indian corporates have substantially risen over the past few years as the appetite for INR has been static in the last couple of years in the international market. Companies with export earnings have aggressively raised foreign debt in their books to exploit the interest differential. LIBOR rates are currently at a historic low.

1. Diebold, Francis. X, Santomero, Anthony M., 'Financial risk management in a volatile global environment', Wharton financial institutions Center, October 1999

What this enhanced volatility bodes for Indian corporations is to measure their FX exposures and have a sound risk management approach towards the same. For companies with high degree of FX exposures, be it in the nature of trading/operating or borrowing exposures, the FX market volatility may be sufficient to wipe out the entire operating profitability and it becomes more pertinent to address the same. Further, the Reserve Bank of India (RBI) tightened provisioning norms for commercial banks with respect to their loans to corporations that have un-hedged foreign exchange exposures. The extra capital required to be kept aside by lenders would imply a higher cost of borrowing (as penalty) for corporates that refrain from hedging (or lowering) their FX risk.[2]

Consequently, corporations have increasingly been going back to the drawing board to re-assess their need to hedge their FX risk, embedded in their trading and loan exposures, using financial instruments such as currency forwards or options. Moreover, the question of how much to hedge and for what tenor confronts many corporate treasurers as companies may not want to lose out to competition just because their portfolios were over-hedged compared to industry peers, or to miss out on the current opportunity of locking in profits on their exposures. Further, the forward premium in case of USD INR transactions is also quite volatile and is dependent on the market expectations of currency and interest rates [Chart 2]. Exporters receive the forward premium while importers pay this as a cost of hedging their exposures. With most hedging decisions being reviewed 'post facto', there seems to be a widespread reluctance to take bold decisions.

Chart 2: USD INR forward premium for various tenors

Source: Bloomberg

Any existing 'natural hedge' relationship in case of offsetting FX exposures (like a company having both inflows and outflows of the same foreign currency) should be identified. The combination of suitable financial instruments (for e.g. forwards, options and swaps) of hedging and hedging strategies (such as instituting target and stop-loss levels) could help ensure effective risk management with a potential for upside participation in case market moves in favour. Further, in case hedging also covers forecasted exposures, the accuracy of forecasts becomes critical as any adverse market movements may lead to inefficient hedging and losses to the organisations.

Further, large exporters with foreign currency inflows may create liabilities in the same currency by raising foreign currency loans/ECB and matching the flows with loans' interest and principal repayment schedule to eliminate any FX risk. Companies with healthy credit ratings can access funds at a very cheap rate (e.g. LIBOR + 200 bps) versus rupee sources of funds like cash credit or term loans which may typically cost 11 to 13 per cent. Few large exporters also go a step further and create synthetic USD loans by using currency swaps on their existing rupee term loans to reduce the borrowing cost and also remain FX risk neutral.

A balance needs to be maintained and the top management needs to recognise that the primary aim of the risk management activity is not to provide additional cash flows to the company but to protect the budgeted flows. A well-defined risk management policy can not only help ensure predictability of the cash flows but also help in reducing management time spent on the process.

While there could be an urge to foresee the future and beat the market, more and more companies are rightly realising that it is better to be prudent and hedge exposures in a disciplined manner as per policy rather than taking calls on the currency movements based on market forecasts.

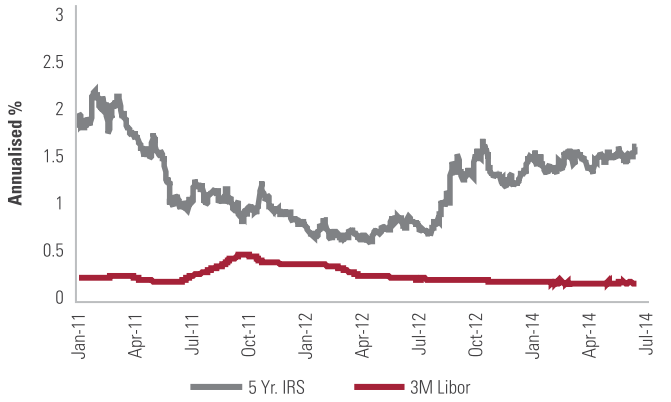
Interest rate risk: Managing borrowing costs

USD Libor interest rates have also been behaving uneasily with the US Federal Reserve Bank alluding to a change in its stance on the accommodative monetary policy after a complete withdrawal of its quantitative easing measures. Hardening of bond yields in the US saw sell offs in the emerging market as the 'risk adjusted yield' differential between the US and emerging economies narrowed.

Interest Rate Swap (IRS), which can be considered as the benchmark hedging rate for floating to fixed swaps (in the same currency) to hedge pure interest rate risk has been quite volatile [Chart 3]. IRS normally is a leading indicator on the movement of interest rates and is derived from the forward rates or markets expectation of the LIBOR in the future. Consequently, the cost of hedging also increases and the corporate treasurer has to take a call on locking the floating rate liability. Larger organisations are likely to give more emphasis on certainty of cash flows thereby requiring them to convert their floating rate liabilities to fixed rate. Even though the ideal mix of fixed-vs-floating debt varies across companies based on their risk tolerance and market access, a formal guidance should be provided by the policy.

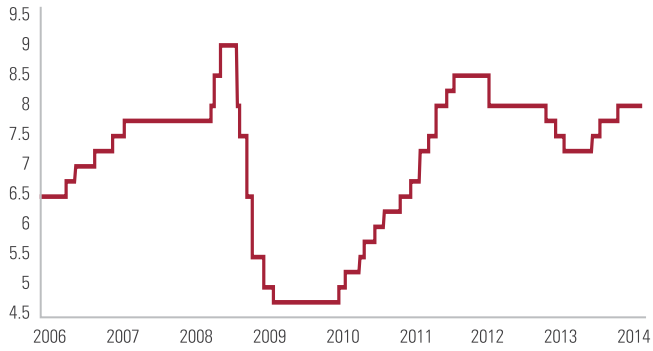
2. Gautam, Ashok, 'Forex markets and currency derivatives', FICCIFinancial Foresights, Vol-4 Q2 FY13-14

Chart 3: USD Libor and swap rates



Source: Bloomberg

Chart 4: RBI repo rates



Source: Global-rates.com

Further, rupee borrowing costs have also remained at elevated levels with the RBI still not comfortable in reversing the high interest rate regime anytime soon due to inflation concerns [Chart 4] . Corporations seem to be facing a serious challenge in getting access to funding at reasonable rates to finance both their working capital needs and capex.

Hence, newer avenues of fund raising have been explored by many corporates as they cannot afford to simply rely on the traditional sources of funding in the dynamically changing credit space. The lack of depth and liquidity in the corporate bond market poses a big challenge for the Indian corporates and they tend to look abroad for the same.

Some other innovative methods to reduce borrowing costs are in the form of structured trade finance deals which may include creating a 'bankruptcy remote' SPV at arm's length to delink the credit rating from the sponsor enabling access to credit at favourable rates or tranching of assets to attract different class of investors. Getting a third party guarantee is also means of credit enhancement to access cheaper credit.

Commodity Price risk: A lesser known evil

Commodity risk has been perhaps the least focussed area in financial risk management despite it constituting a significant component of the risk exposure for many organisations. In firms that do manage their commodity risk, it does not form a part of the core treasury function but rather resides with the supply chain/procurement team. Surprisingly, commodity price risks are not adequately identified (let alone measured) despite the fact that many manufacturing companies run a large quantum of direct or indirect exposure to commodity price risk by the nature of their raw materials or finished products. Almost two-third of companies surveyed in a KPMG survey[3] claimed to have no specific guidance on commodity price risk management.[4]

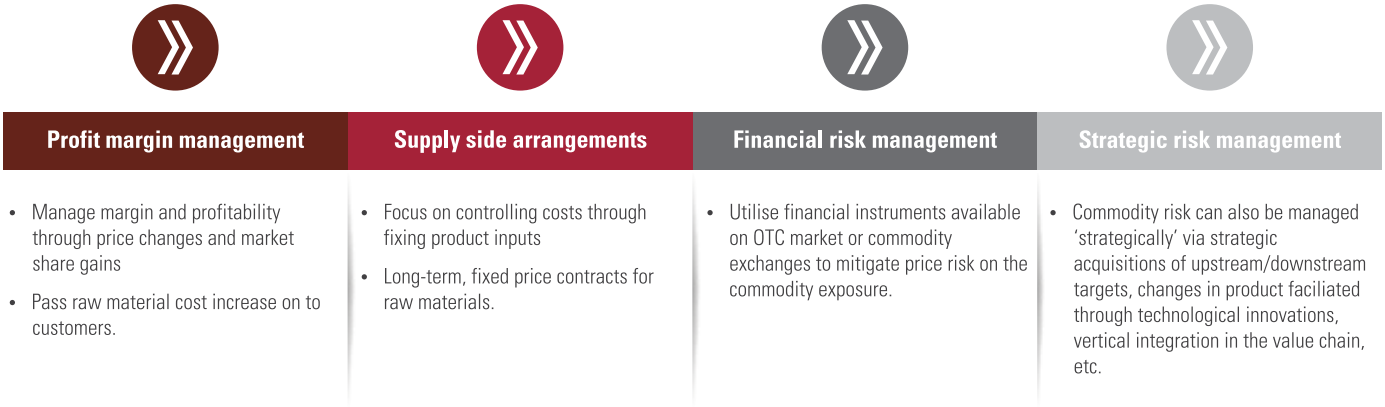
The lack of capability for commodity risk management cannot be denied as it is a complicated subject requiring an appreciation of numerous factors, nuances of correlations in physical commodities, longer term supply-demand issues, basis-risk (difference between spot and futures prices) and the physical supply chain. However, increasingly, large corporates have been using various techniques to manage the commodity price risk by actively negotiating on fixed price contracts, passing on the price risk to the consumers or using financial instruments like commodity futures on global/ domestic exchanges to hedge the price risk [Chart 5].

We have witnessed high volatility in almost all key commodity prices viz. Energy (Oil, Natural gas and coal), metals (Copper, Aluminium, and Zinc) and agri- commodities (rubber, sugar, etc.). Perhaps a pertinent example could be the current crude oil price slump wherein Brent crude fell sharply from USD 110/ bbl to below USD 60/bbl. This directly impacts the oil refining companies where crude oil is a raw material and indirectly other organisations which use oil distillate products like gasoline, bitumen, etc.

While many commodities have active products being traded on the global exchanges like LME, CME, CBOT or domestic MCX, many others may not have any traded products. They are then hedged using similar products which have high degree of correlation with them or alternatively through pricing agreements with the supplier/ buyer (as the case may be)

3. 'Managing Currency and commodity risk', KPMG India Survey,2013
4. Lester, Kevin , Haigh Alexander, 'Commodity and FX risk management- An integrated Approach', TMI, Issue 187

Chart 5: Commodity price risk management approach



Source: xxxxx

A vibrant and equipped treasury to manage financial risk

For treasury to serve as a value add and strategic partner to the business, it should incorporate some of the following key elements:

1. Treasury policy manual: A thorough and up-to-date treasury/financial risk management policy can go a long way in protecting against the volatility in earnings, cash flow and shareholder value. Greater the flexibility available under a company's risk management policy, greater is the chance of a company to be exposed to unwanted risk. On the flip side, a very stringent policy could also result in the company losing out on favourable market opportunities. Recognising this, many of the large corporates have moved from a 'deterministic' to a 'stochastic' hedging process whereby the treasury actively tracks the market and business situation to arrive at suitable approach within the broad ambit of the treasury policy.
2. Centralisation: Treasury is a highly specialised function and there was always a dilemma as to whether risk should be managed at the unit level or at a centralised level. While decentralisation provides more autonomy to individual business units, given the high volatility and development of complex derivatives, companies are moving towards centralisation of this function where they can concentrate and utilise their resources.
3. TMS: A robust treasury management approach is critical for financial risk management of the treasury, provides transparency and improves internal control. Companies utilise the treasury system to simulate the impact of different risk scenarios, provide adequate management reporting and integration with accounting and other business functions. Automation in the routine treasury operations reduces the human operational risk and enhances efficiency of the routine processes. Further, suitable reporting mechanism should be put in place for a good control over the exposures and effective decision making.
4. Regulatory compliance: Treasury should also keep a track of the pertinent regulatory changes in the financial space which may be relevant to their decision making process. For e.g. the RBI had introduced a slew of measures to control the free-fall in rupee last year like restrictions in forward contract bookings and cancellations to discourage speculative trading. In the past, companies that involve strong international trade have known to indulge in trading activities and there have been instances where healthy companies were on the verge of going belly-up purely due to derivative losses. It needs to be determined that treasury operates as a risk management and strategic centre of excellence and should not add any risks by virtue of its actions. The treasury has the ownership of compliance to the regulatory regime and internal policy guidelines.

Conclusion

Needless to say, financial risk management as a function is viewed more positively now, holds high level of influence within the organisation and is an essential source of competitive advantage.

It is understood now that the volatilities of various asset classes are here to stay and firms need to be prepared for it by investing in a professionally competent and technically equipped treasury to guide them through the rough patches.

Emergence of cybersecurity and data privacy risks in a digitally enabled enterprise

Atul Gupta
Partner, IT Advisory, KPMG in India

Changing face of cyber security

The first attack on technology was recorded in France in 1820 where employees of a textile manufacturing loom engaged in disrupting acts to dissuade the manufacturer to use a new technology that would allow recurrence of steps that run in succession in the knitting of special textiles. The situation was handled, deploying additional mill guards and rounding up the dissenting workers. An archaic solution to an emerging problem.

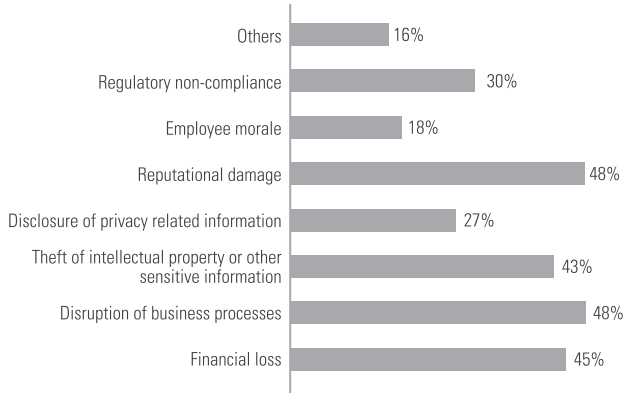
Since that era to 2015, these attacks have become sophisticated and multiplied significantly in number (riding on the wave that has connected the world ,i.e., the internet) and continue to grow further in magnitude and scope.

Leveraging dynamic malware, complex web attacks and a gamut of other tactics; cyber criminals and hacker activists are becoming more erudite and effective in their efforts to steal and disrupt sensitive information. And as we shift gears to being a knowledge economy with companies outsourcing their business processes to partners, moving data and applications to 'the cloud' and embracing social media to communicate with their customers and collaborate with their suppliers, securing the requisite cyber environment is only going to get exponentially challenging. In the given environment, one of the key emerging requirements is to have an effective incident management process which can enable companies to effectively respond.

Board room agenda

Cyber-attacks and data breach; accidental or intentional are globally diffused and financially driven acts, which are not limited to any specific sector or organisation. A multitude of companies of different sizes and across sectors have been victims to this crime. Cyber warfare, cyber-attacks sponsored by state actors, can go beyond business interruptions and the destruction of strategic data and can re-define an organisation's brand in a fraction of seconds. It includes cyber espionage, intellectual property loss, confidential data theft, as well as significant externalities for third parties.

Impact of cybercrime in India



Source: KPMG in India Analysis - Cybercrime survey report 2014

'According to the survey results, 48 per cent of the respondents indicated that they suffer disruption of their business processes and reputation damage as a result of a cyber-attack. These have often led to financial losses (either direct or indirect) as indicated by 45 per cent of the survey respondents.'

The last decade has seen an enormous increase in the activities of individual hackers and specialised cyber criminals. The high profile security breaches that took place in 2014 have been a serious concern among the board members across organisations. As more and more attackers target deep-rooted retailers, media companies and financial institutions, infiltrating their computer networks and gaining access to sensitive information, Cyber Security and Data Privacy has become a significant concern for boards. Many companies and organisations are recognising and experiencing first-hand the fact that cyber-attacks and privacy ruptures are no longer a matter of if but when[1].

> "Security is not a one-time activity, it is an ongoing process."

Cyber security is being recognised as amongst the top enterprise level risks which global organisations face today. Investors and regulators are increasingly challenging boards to step up their supervision of cyber security and data privacy and are calling for greater transparency around major breaches and their impact on the business[1].

Data Privacy: Is it given due importance?

With the focus on cyber security emerging across companies, there is often a view that data privacy shall be addressed as part of it. The leaders need to understand that with the advent of new and innovative service delivery models like; cloud and total outsourcing, organisations are under tremendous pressure to ensure privacy in addition to security[4].

Several regulating bodies across the globe have taken significant measures to ensure privacy of sensitive information is maintained.

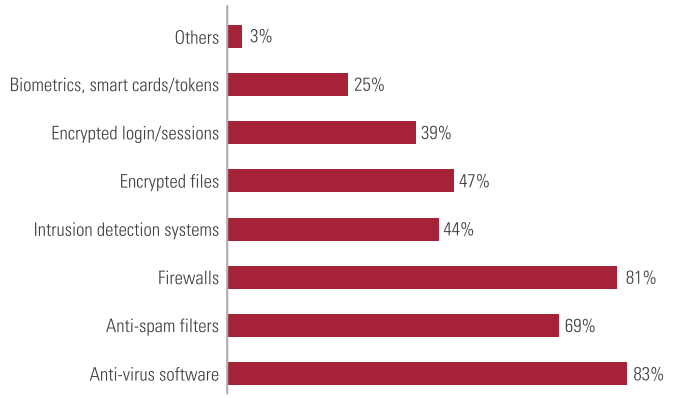
- European data protection legislation has formulated a set of cross-border principles governing the transfer of sensitive and personal data outside Europe. Under the law, personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data[3].
- US has acts for data privacy, including Health Insurance Portability and Accountability Act (HIPPA) released in 1996 which aims at safeguarding individually identifiable healthcare information and helping the healthcare industry control their administrative costs. The act lays guidelines for security of electronically processed health information.

However, one challenge which exists is that the data privacy legislation around the globe is inconsistent with some countries having a highly restrictive framework while others being on the other extreme. Such discrepancy makes the task of protecting privacy of information in a globally connected world even more challenging and this at times becomes a non-tariff trade barrier.

While the government and regulators may not always be able to come out with specific laws and regulations in line with changing industry practices, it becomes the responsibility of business leaders to ensure that the risk profile of the organisation is holistic and also takes care of the risks emanating from the business operating model[4].

According to a survey conducted by KPMG in India, a few respondents indicated that their organisations are doing their bit to realise a secure environment, while others are still lagging behind when it comes to enhancing their internal cyber security and data privacy infrastructure.

Security measures



Source: KPMG in India – Cybercrime survey report 2014

Ensuring security and privacy is a process and not a solution, and preserving IT networks and sensitive data from electronic attack and exposure, both from the internet and internally at organisations must be a constant endeavour.

1. KPMG- Audit Committee Institute – GBI – The Cyber Security Challenge
2. KPMG – The five most common cyber security mistakes
3. http://www.out-law.com/page-8170
4. Being Compliant – Demystifying Role of IT

Regulations and standards

Various frameworks and guidelines have been released by nations across the world to help companies irrespective of the magnitude of cybersecurity risk or level of cybersecurity adaptation to apply rules and leading practices pertaining to risk management and achieve the desirable security and resilience of important infrastructure.

In the U.S., the National Institute of Standards and Technology (NIST) worked together with the Homeland Security Department and stakeholders from the industry to develop a set of acknowledged and publicly confirmed standards that can be used to identify, detect, safeguard, respond to, and recuperate from threats.

In India, the government released a National cyber security policy with the aim to monitor and protect information and strengthen defence. The IT Act continues to be a guiding act for driving security and privacy environment across organisations (Article 21 of the constitution - right to life and personal liberty and the privacy rules propagated as part of section 43A of the IT Act are considered to preserve the right to privacy). In addition there are specific regulators who have mandated specific frameworks and control environments for companies to ensure that security and privacy is maintained.

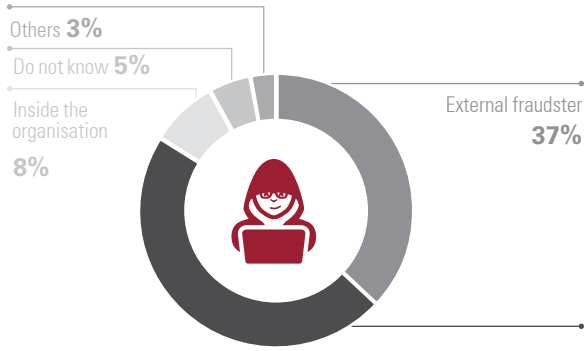
Despite the regulations and acts, the challenge for India continues, where the awareness among citizens about the importance of data privacy is still low.

Proposed framework and conclusion

In the current culture and environment of extensive information sharing, it is inevitable for businesses to have continued exposure to security and privacy threats. These are amplifying with the adoption of newer technology trends including cloud, m-commerce, BYOD and other contemporary techniques.

With the attacks being more advanced and persistent it has become mandatory for organisations to integrate a sustainable cyber design model.

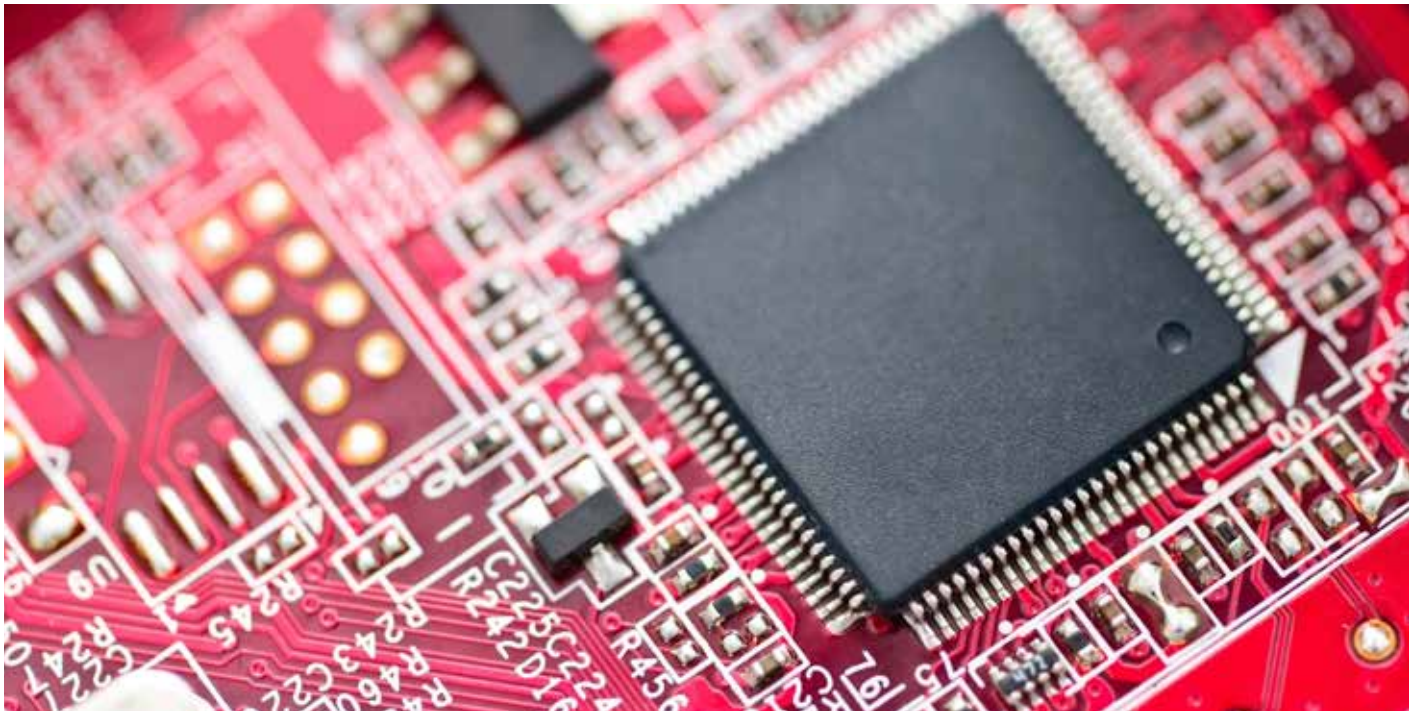
Profile of cyber attackers



Source: KPMG in India Analysis - Cybercrime survey report 2014

The risk of data loss stems from both in-house and external threats, including mismanagement of the device itself, external manipulation of software vulnerabilities and the deployment of unreliable business applications.

Consequently it is imperative that organisations need to have a holistic framework to address the insiders with malicious intent or professional intruders constantly seeking access to sensitive information. A suggested framework for building a sustainable model for cybercrime risk management is outlined as follows:



Suggested framework for managing cybercrime risks

Source: KPMG in India Analysis - Cybercrime survey report 2014

> 100 per cent security is an illusion, and chasing that 100 per cent target will lead not only to frustration but also to a false sense of security[2].

Doing business securely in the era of cyber-crime and espionage is definitely a challenging task. However, embedding an information classification scheme, and with it a 'need to know' cultural change can help organisations avoid these malicious acts. The adage 'Prevention is better than cure', holds significant value for organisations trying to fight the cyber warfare and protect their data, along with a robust incident response plan.

Digital forensics

Sandeep Gupta
Partner, Forensics, KPMG in India

As organisations, governments and individuals increasingly leverage technology for conduct of business, they are also increasingly exposing themselves to the threat of digital fraud. Digital fraud comprises of a range of illegal activities using computing and communication devices aimed at causing loss to organisations. Digital frauds could range from fund embezzlement to activities like data theft, intellectual property violations, etc. Given the nature of technology and its usage, such wide range of frauds can arise in any part of the daily business operations, be it banking, sales, procurement, finance or administration. The pervasiveness of potential frauds put organisations at serious risk of significant business impact.

Trends in digital frauds

As part of the recent KPMG Cyber Crime Survey 2014 revealed that 49 per cent of survey respondents have experienced cybercrime and digital frauds in the past 12 months. With more and more businesses increasingly adopting technology and e-commerce, and criminals having access to greater cybercrime tools, the number of such incidents can only be expected to rise in the future. With the recent spate of digital incidents ranging from leaked personal information of celebrities to confidential information disclosure of large organisations, the media attention on digital forensic services has significantly increased.

From a digital fraud risk mitigation standpoint, though it is seen that organisations increasingly are becoming aware of the possibilities of digital fraud with in their business environment, a proactive approach to risk management has not been forthcoming possibly due to:

- Limited understanding with the operational management teams on the potential impact of the full range of digital frauds
- Lack of top management support in building digital defenses for effective risk management
- Lack of procedures to determine timely capture of digital evidence and maintain it
- Inadequate skills available within the IT team to identify, investigate and manage digital fraud cases
- Minimal understanding of digital evidence related laws in India.

Types of digital frauds : A quick overview

With computers and mobile devices being all pervasive in the business environment today, digital fraudsters find it all the more beneficial and easier (depending on the defense mechanisms in place) to perpetrate crime. As in cases of many crimes/fraud, the root cause of digital fraud is often a mix of three core elements, namely: opportunity, pressure and rationalisation that influence the digital fraudster. Bearing this in mind, it would suffice to say that digital frauds occur in various ways depending on the motive and opportunity available to the digital fraudster.

- Data theft/destruction: These cases typically involve employees using laptops, USBs, web shares, emails to leak out company sensitive information like financial statement, technical designs, intellectual property (like patents), payroll information and customer databases. This set of digital crimes also involves critical business data being destroyed to make it unrecoverable for genuine business users (e.g. deletion of critical negotiation emails, quotation calculations, proposals, soft copy of agreements by exiting employees or a malicious hacker). Digital fraudsters these days also use custom developed malware as a tool for data theft and data destruction as it goes undetected by many anti-virus softwares and can be controlled remotely without the fraudster actually entering the victims network or computer. Several fraudsters have even started blackmailing organisations by threatening to leak the information in public domain and demanding ransom money in form of bit coins.
- Email frauds: Frauds using emails has become rampant; it ranges from employees using email credentials to log into their colleagues' email accounts or false implications to spoofing, spamming, phishing with a view to defraud their recipients.
- Online/Digital defamation: With businesses leveraging the internet and social media to gain an edge in today's consumer focussed market, a typical fallout is that employees without authorisation communicate on such platforms to carry out unauthorised communications/ posts (e.g. tweets). Many a times, employee accounts are hacked to post such comments. Such cases lead to immense reputation loss to the targeted organisations.
- Financial embezzlement: This instance of fraud normally involves usage of official devices to access ERP, online banking and customer/vendor communications to commit a variety of financial crimes such as teeming and lading, vendor kickbacks, payment diversions, invoice falsification, financial statement reporting frauds, etc.

Digital forensics: A tool for effective fraud detection

Based on the types of frauds mentioned above, it is evident that fraudsters these days prefer to carry out illegal activities using computing and mobile devices, making it hard for companies and investigators to establish culpability. In order to detect digital frauds, organisations are increasingly leveraging on digital forensics to bring out the accurate facts of the case.

Digital forensics encompass the recovery and forensic review of content found in computing devices (servers, laptops, mobile phones and PDAs), following standard procedures acceptable in a court of law. These days, digital forensics is often being used in criminal or civil courts to support or refute a hypothesis. It is also used extensively during fraud investigations or cyber attack investigations (for example, investigating a system breach which occurred from outside or loss of customer data).

Following are the broad areas on how digital forensics can help and ways for organisations and investigators to extract evidence for effective legal re-course:

- If correct acquisition procedures are followed, it ensures that the data is acquired in a manner that is compliant with local information technology, PII (Personally Identifiable Information) related regulations and is admissible in the local court of law
- Ensures that the no critical/clinching digital evidence is inadvertently destroyed at the time of responding to the events
- Helps in recovery of undisclosed/hidden evidence that is used or part of committing such frauds
- Helps in recovery of deleted evidence that is used or part of committing such frauds
- Identifies communications that may be relevant to the fraud committed
- Identifies digital foot print of the fraudster
- Provides corroborating information pertaining to time line of frauds.

Digital forensics on computing devices can be carried out using different techniques, the nature of techniques to be employed depends upon the information to be obtained. An overview of some of the commonly used techniques for digital forensics is as under:

- Image Analysis: Device image analysis encompasses performing acquisition and investigating artifacts such as computer systems, mobile devices, storage mediums, electronic documents, embedded systems, industrial control systems, static memory devices, etc. by acquiring a replica (image) of the target data in read-only mode. Image acquisition can be done in one of the three manners:
  - Physical acquisition - bit-by-bit copying of the entire physical data from the target device
  - Logical acquisition - copying logical storage partition of the target device
  - Targeted acquisition - copying specific pieces of electronic data from the target device.
- Digital Examination: Certain forensic activities can be performed without the need of an image acquisition. Activities such as network traffic capture, audit log analysis, breach incidence response, email header analysis, malware analysis, trend analysis, etc. can be performed without necessarily acquiring forensic images. However, a limitation of such analytical activities can cause difficulty in proposing, testing and concluding hypothesis as part of the investigation.
- In-memory Forensics: Memory forensics is primarily used in investigating advanced computer attacks such as malware or botnet attacks, which are sophisticated and stealthy enough to avoid leaving data trail on the affected computer systems e.g. APT (Advanced Persistent Threat) malware. Consequently, the RAM memory must be analysed for investigation.

The following table illustrates (this is not an exhaustive list) how digital forensics can help in various investigative scenarios by recovering critical data.

Sr. No.	Type of fraud	Types of evidences that can be recovered for legal recourse
1	Data theft/destruction	• Recovery of deleted data • Recovery of hidden data • Names of files transferred to portable devices • Indicators of data stealing malware and remote C&C (Command and Control) servers they transmit to • Presence of key stroke loggers and C&C servers they transmit to • Data share websites visit history • Details of data wiping tools installed and used • Data sent to personal accounts using official emails
2	Email frauds	• Email origination details (indicating aspects such as whether it is from within office network or external network) • Email accounts and passwords • List of online email accounts accessed • Recovery of deleted emails from the email client • Data sent to personal accounts using official emails
3	Online defamation cases	• Content used for defamation/harassment (media, files, images, etc.) • Recovery of deleted content used for defamation/harassment • Internet history of access to sites for conducting defamation activities • IM/chat histories used for online abuse/defamation • Recovery of deleted malicious emails sent as a part of defamation activity • Email origination details (indicating aspects such as whether it is from within office network or external networks) • In case of mobile devices, artifacts such as- – Call history – Texting history – Mobile browsing history – GPS logs (if provided by in-built applications)
4	Financial embezzlement	• Email communications that can be retrieved from digital images based on investigation case key words that could indicate potential embezzlement • Content discovered that can be retrieved from computer images based on investigation case key words that could indicate potential embezzlement • Personal artifacts stored unauthorised on official devices (that could indicate/point towards wrong doings especially in kick back cases – the admissibility and right to view will depend on local laws pertaining to PII in case of international cases) • Digital log analysis reveals traces of how and when the event took place. It is an important piece of evidence which cannot be neglected. Organisations may not have audit logs turned on, however various applications, databases and systems have its own logs which can be leveraged on.

Digital forensics role in effective enhanced risk management

Digital forensic efforts are greatly enhanced if the organisation has appropriate audit trails and logging mechanisms established in its business environment. However, it is common for organisations to not have proper audit logging and monitoring practices implemented. Lack of system level audit trails generated at the time of business activities/ transactions can hamper the investigation as digital forensic cannot recover something not created in the first place. It becomes difficult to propose/test hypothesis without having appropriate audit trails to substantiate the analysis.

Challenges to digital forensics

With the Companies Act, 2013, laying emphasis on fraud risk management and fraud reporting on the management and auditors, it has become vital for information technology departments to deploy forensic controls in IT systems and IT processes to facilitate an amicable environment for digital forensics, should the need arise. Though most IT departments are now waking up to this reality, the challenges many IT departments face are listed below:

- Identifying what system/data is relevant for the coverage of IT forensic controls
- Systems/Data to be covered that may be complex
- Limited infrastructure for managing forensic information, evidence and control logs
- Limited technical knowledge of IT support staff.

Insights

Typical forensic control lapses:

Appropriate IT controls (or lack of) in the business environment also proves to be a key factor in digital forensic process. For example, lack of IT control over end-user application installations can allow a malicious employee to install anti-forensic tools (such as secure deletion programs) for hiding their tracks. IT staff may also have the perception that data backup is equivalent to a forensic image, thus secure wiping the system without obtaining prior approvals, this can be disastrous in case digital evidence needs to be recovered from such wiped laptops. Some other typical forensic control lapses that allow digital fraud incidents to take place or hamper digital investigations are listed as under:

- Anti-virus controls are switched off on desktops
- Anti-forensic tools such as registry cleaners are permitted to be installed
- End users have the ability to switch off OS based Firewall software
- End users have the ability to clear/delete event logs
- Absence of robust incident management controls (e.g. classical example of weak incident response would be a case of infection alerts by the anti-virus system. A typical IT support response to a malware infection would be to clear the infected PC/server and to ensure timely availability of the systems. However, seldom do IT teams carry out a proper root cause assessment to understand the to mode of infection, the behavior of the malware the impact on the system, whether any critical data was stolen, destroyed, etc.

How can organisations build stronger controls to facilitate and manage digital evidence?

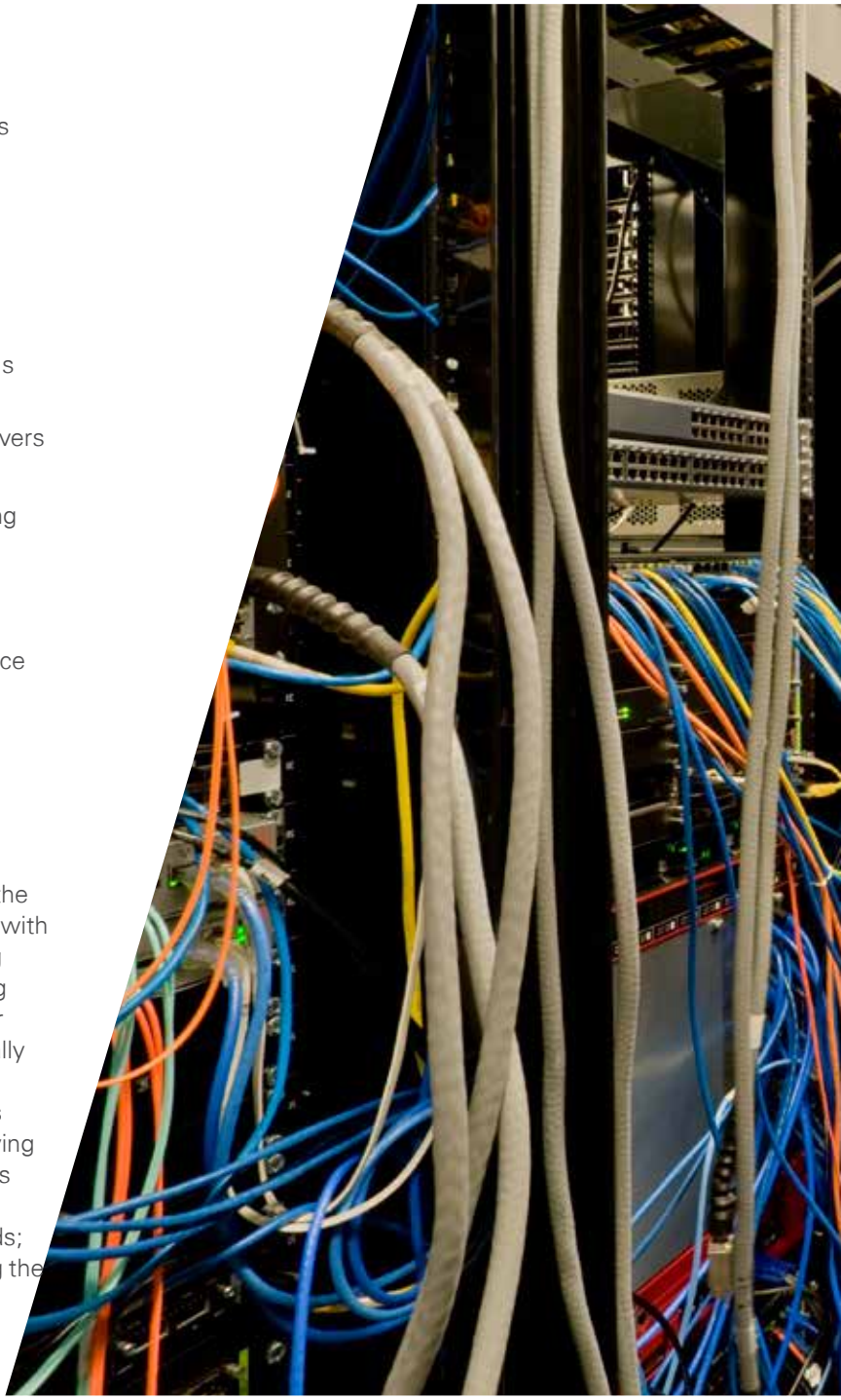
Due to compliance requirements, CIOs have now realised that forensics controls are vital to determine the accuracy of management reporting of fraud incidents is adequately supported by the right digital data. This thrust is now translating into CIOs seriously enhancing IT risk management practices by introducing forensic controls. Key action points CIOs must take to determine that the right forensic controls are designed and implemented are as under:

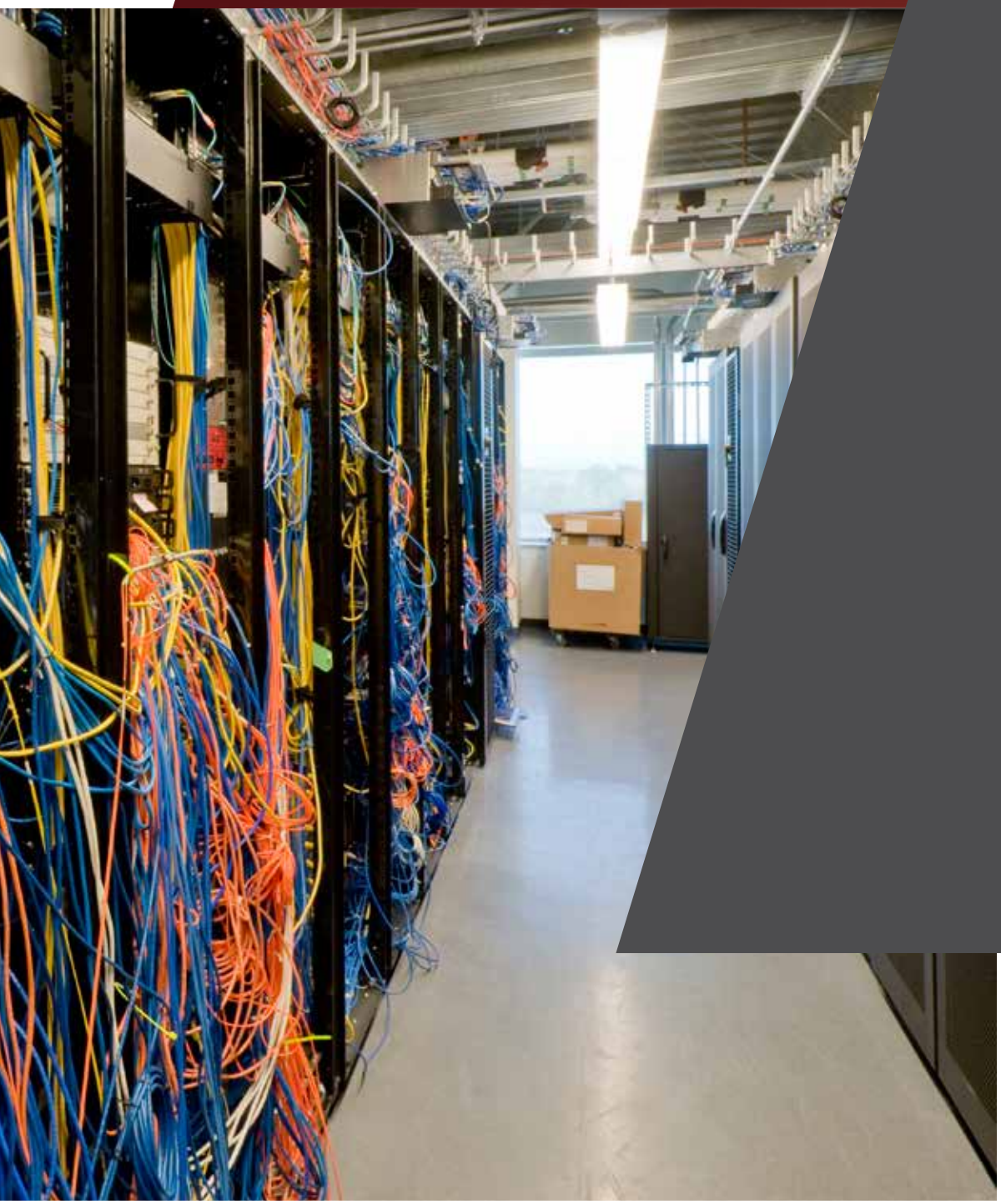
- Understand the fraud risks that can impact business operations (jointly with business owners)
- Identify IT systems that can be used to perpetrate the same or are incidental to the same
- Identify information that can help in detection of digital frauds (identifying key log points and information stores that can assist in digital forensics)
- Formulate data patterns/alert rules of behaviour or relationships that might alert the IT/business team of irregular and suspicious behaviour (e.g. SIEM rules for alerts generated in case of device logs from network gateway indicate data breach)
- Understand in detail the evidence impacting legislations like IT Act (Amendment) 2008, Evidence Act
- Build an effective incident response framework that covers key processes like:
  - Incident Monitoring and Incident Response (including first responder procedures)
  - Evidence gathering procedures (including integrity checks and evidence shipping)
  - Evidence Chain-of-Custody procedures (in accordance with evidence related legislations).

Conclusion

The field of digital forensics is gathering increasing prominence as part of fraud investigations. While a key objective of digital forensics is to recover evidence of a criminal activity that has acceptability in the court of law, the evidence obtained from computing devices can also help with other areas of investigation. In an effort to fight increasing digital fraud incidents, digital forensic is increasingly being incorporated by law enforcement agencies as part of their infrastructure. In the private sector organisations, especially in the financial sector, have either begun to build in-house digital forensic teams or contract third party organisations on requirement basis. Digital forensics is constantly evolving and adjusting to meet the demands of newer technologies being released in the digital world. The capability of digital forensic investigation tools has grown by leaps and bounds; with such advancements the methodologies for obtaining the information have also evolved to be more advanced.

Forensic controls in IT systems and processes is a good starting point for managing risks, periodic monitoring of fraud risks and evolving IT forensics controls to match the changing landscape of technology and data complexities is vital to determine so that the organisations stay protected and have effective means to facilitate digital evidence, if required. The positive effect of such a dedicated exercise would mean that organisations would effectively manage fraud risk from a technology standpoint and should they be impacted, they have the effective wherewithal to ensure that the fraudsters are brought to book and the impact of fraud is reduced.





Increasing stakeholder scrutiny of climate change and sustainability related risks

Santosh Jayaram
Director, Sustainability & Climate Change, KPMG in India

Introduction

There is now unequivocal scientific consensus that the earth is experiencing a significant change in global climate. The effects of this change on planning and operations of business for government and organisations will be significantly high (Kolk and Pinkse, 2008)[1]. Various key climate shift patterns to be observed in the future include higher temperature, shift in rainfall patterns and extreme events such as droughts, heat waves and storms. These climatic events pose risks to multiple organisational stakeholders and thereby to the functioning of organisations. When managing climate change and sustainability risk, organisations cannot rely on the stability of the climate to be in harmonisation with trends observed in the past 50 or 100 years. They need to consider that the climate will progressively differ from the climate today in many ways. Climate change will probably have pervasive effects on the functioning of an organisation and the expectations of stakeholders. While past experience of climate patterns and its forecast may be valuable in forming climate risk strategies, the effects may be different for different time scales. This will also change the expectations of stakeholders of an organisation in the way an organisation manages the climate change risks.

Warming trends and increase in temperature extremes have been observed across most of the Asian region in the past century (IPCC, 2014)[2]. Changes in precipitation trends, including extreme precipitation events, have also been observed with both increasing and decreasing trends in different areas and seasons. This poses several challenges across the region. For example, climate change linked water scarcity is expected to be a major challenge for the region, similarly impacts on food security and production also pose a major threat across Asia, where many regions will experience decline in productivity. Especially in the Indo-Gangetic plains there could be a decrease of about 50 per cent in the productivity of the most favorable and high yielding wheat area. Costal and marine systems will also experience direct stress from the climatic drivers. The costal water levels will have exponential rise due to the expected rise in the mean sea level thereby disturbing the existing coastal infrastructure. (IPCC, 2012).[3]

Probably climate change will adversely affect the sustainable development of most Asian developing economies. Extreme events can also have a significant impact on human health, livelihood, and poverty in different magnitudes depending on the geographical positioning. A ripple effect of these changes would be seen across sectors, particularly in the context of resource utilisation and competition.

1. Kolk, A. and Pinkse, J. (2008). Business and climate change: emergent institutions in global governance. Corporate Governance: The international journal of business in society, 8(4), pp.419-429.
2. IPCC, (2014). Climate Change 2014, Mitigation of Climate Change. Cambridge, New York: Cambridge university press.
3. IPCC, (2012). Managing the risks of extreme events and disasters to advance climate change adaptation. Cambridge, New York: Cambridge university press.

Understanding the link between Climate change and Risk

Organisations may not have a direct impact from climate change, however the chain of consequences may directly affect its performance with respect to its customers or other stakeholders. Various biological, economic and social impacts can cumulatively be linked to changes to multiple climate variables and thus drive other impacts on functioning of organisations. For example, droughts are linked both to increase in temperature and decrease in rainfall, similarly floods are often linked not only to the regular flooding season but also to the sudden extreme conditions linked to climate change. It is thus essential that organisations and governments identify the various entities and services that are at risk from climate change. Various approaches like mapping of entities and services sensitive to climate change can be employed for effective visualisation and implementation.

The approach to manage climate change risks generally involve defining a clear boundary on the projected climate change, however this is subject to huge uncertainty that arises because although climate change is well established, the actual magnitude of the change is not precisely defined (Haque and Deegan, 2010).[4] Furthermore, decision makers also face a dilemma in defining the boundary of assets and activities which will be impacted by climate change and the costs of these impacts for the organisation. However, identification of the assets that may be affected by climate change can be achieved by developing climate change scenarios over different geographical regions and timescales. These scenarios provide a means to assess the impacts of climate related risks across different organisations. For example, historically, Rotterdam's advantage has been its location on the delta of the Meuse and Rhine rivers, making it home to one of Europe's busiest shipping port. However, with 90 per cent of the city sitting below sea level, Rotterdam faces significant obstacles to stay afloat in the face of sea-level rise and flooding brought on by climate change. The city is turning this challenge into an opportunity to become a global leader of water and adaptation innovation through its mission to become '100 per cent climate proof' by 2025 (KPMG, 2013).[5]

Rotterdam is steering its climate adaptation initiatives with public engagement, cutting-edge research from its local institutions, and subsidies to incentivise 'green' practices among its 600,000 occupants. A central objective is the 50 per cent reduction of harmful CO2 emissions by 2025. To that end, sustainable transportation policy has given cyclists right of way in traffic, with separated paths to privilege bicycles. In an effort to support rooftop gardens, which absorb CO2 and rain, and reduce the urban island temperature effect, the city offers a 50 per cent subsidy for their construction. Since 2008, there has been an average of 40,000 square meters of rooftop gardens constructed per year (KPMG, 2013).[6]

To control the future effects of extreme flooding the city has invested in a range of innovative rainwater storage solutions. For instance, a newly built parking garage incorporates a 10,000 cubic-meter underground rainwater store. Another solution involves stratified public squares that serve both as community centers and water stores during heavy weather. New floating communities on the waterside near the coast are not only architecturally innovative but also attractive to new businesses. (KPMG, 2013).[7]

These scenarios can be developed by analysing the climate change data on a broader scale using meteorological records and by gauging the geography in line with Intergovernmental Panel on Climate Change (IPCC) guidelines. The risk arising from a particular climate change scenario must be considered and described. Furthermore, it is also essential to develop a model which reflects the impact of climate change on key performance indicators for a long time horizon. Such a process can be used to forecast climate change risks on various activities and assets of an organisation, thus resulting in a systematic decision making tool for organisations and governments. (IPCC, 2012).[8]

Measures taken to mitigate impacts of climate change by an organisation may be subject to scrutiny by stakeholders; this has both positive and negative impacts. Thus systematic climate changes related measures must be incorporated in the policies of an organisation. With recent changes in the global dynamics of climate change, governments are instituting several action plans for mitigating and adapting to climate change. Organisations must devise strategies for identifying the risks and opportunities of increased scrutiny in the climate change arena (Galbreath, 2009)[9].

By publicly committing to a programme's objectives an organisation may invite increased stakeholder scrutiny, however this also presents the organisation with an opportunity to gain positive public recognition. This stakeholder scrutiny can act as the primary incentive for organisations to aggressively commit to becoming a sustainability or climate change champion and thereby becoming a market leader. Such commitment also helps in increasing the investor's ratings for an organisation, for example a better performance in the Dow Jones sustainability index may lead to the organisation becoming more attractive to investors.

4. Haque, S. and Deegan, C. (2010). Corporate Climate Change-Related Governance Practices and Related Disclosures: Evidence from Australia. Australian Accounting Review, 20(4), pp.317-333.
5. KPMG, (2013). Rotterdam's climate adaptation – Future State 2030 | KPMG | GLOBAL. [online] Available at: http://www.kpmg.com/global/en/issuesandinsights/articlespublications/future-state-government/pages/rotterdam-climate-adaptation-initiative.aspx [Accessed 4 Janauary. 2015].
6. KPMG, (2013). Rotterdam's climate adaptation – Future State 2030 | KPMG | GLOBAL. [online] Available at: http://www.kpmg.com/global/en/issuesandinsights/articlespublications/future-state-government/pages/rotterdam-climate-adaptation-initiative.aspx [Accessed 4 Janauary. 2015].
7. KPMG, (2013). Rotterdam's climate adaptation – Future State 2030 | KPMG | GLOBAL. [online] Available at: http://www.kpmg.com/global/en/issuesandinsights/articlespublications/future-state-government/pages/rotterdam-climate-adaptation-initiative.aspx [Accessed 4 Janauary. 2015].
8. IPCC, (2012). Managing the risks of extreme events and disasters to advance climate change adaptation. Cambridge, New York: Cambridge university press.
9. Galbreath, J. (2009). Corporate governance practices that address climate change: an exploratory study. Bus. Strat. Env., p.n/a-n/a.

But such scrutiny may also pose a serious risk (Julius, 1997)[10] for organisations that have been disclosing misrepresentative information or using a loosely crafted sustainability and climate change strategy for handing risks because this increased disclosure provides stakeholders with more opportunities to discover and scrutinise previously undisclosed information (Ruggie, 2004).[11] From a stakeholder's point of view this disclosure is considered a good practice as it gives them a better opportunity to forecast future operations of an organisation and take informed decisions. For example; when Nike was accused of relying on suppliers with subpar labour conditions, Nike, released a report emphasising positive information about the state of labour conditions but concealed the low wage information. This improper disclosure drew further strong criticism and scrutiny from activists.

Regions differently affected by climate change will have different response mechanisms and expectations of stakeholders for organisational sustainability and climate change action plans (Johnson, 2003)[12]. A sound sustainability and climate change policy will not only help in addressing the needs of the local variable sustainability and climate change components but also engage with local regulators to address the risks.

A recent example of these strategies was at Holcim, Romania that has committed itself to sustainable development, and integrated the principles of value-creation, sustainable environmental performance, and corporate social responsibility into its business strategy. Working in partnership with its stakeholders, Holcim (Romania) is working to improve the quality of life of its workforce, their families, and the communities within which the company operates. The company's policy and global standards on corporate responsibility are applied to its employment practices, occupational health and safety, community involvement, and customer and supplier relations. Transparent communication, including the annual Romanian Sustainable Development Report (since 2005) helps to build trust and respect of stakeholders. High business ethics and personal integrity also support the credibility and reputation of the company (KPMG, 2015).[13]

Increased awareness among the public and decision-makers about global warming and other environmental concerns has contributed to a preference for products and services that help to alleviate climate change. Apart from producing cement in modern, energy efficient plants, Holcim Romania has also started to use alternative fuels derived from waste. New products with a smaller carbon footprint (Tenco, Structo, road binders) reflect the efforts of the company to produce more cement for the growing Romanian market in a more sustainable way (less CO2 emissions per tonne of cementitious material). In recognition of the company's efforts around the world, in 2008 the Holcim Group was named 'Leader of the Industry' in the Dow Jones Sustainability Index and, for the fourth year in a row, acknowledged as the company with the best sustainability performance in the building materials industry (KPMG, 2015).[14]

In India, under the instructions from the Ministry of Environment, Forests and Climate Change, states are developing action plans for designing activities and programmes for climate change adaptation and mitigation. The state action plans are closely linked with the national action plans on climate change for effective state level implementation (Climate Change Adaptation in Rural India, 2015)[15]. These plans outline the characteristics of sectors and communities that are vulnerable to the impact of climate change. At the policy level, this an initiative which is expected to later lay the foundation for carrying out vulnerability assessments that can assist decision makers in developing methodologies for carrying their own risk assessment in context to climate change and regional geography.

Larger companies are often subject to stronger demands from regulators and public interest groups (Greening and Gray, 1994) and are more often targeted by activists (Eesley and Lenox, 2006) for a stronger stakeholder scrutiny. Stakeholder scrutiny also acts as a catalyst in stakeholders decisions in identifying the credibility of organisations and establishing a policy mechanism (Vial, 2011)[16]. For example, Currently Brazil has the National Policy on Climate Change, which establishes a voluntary reduction commitment of 36.1 to 38.9 per cent of projected GHG emissions until 2020, which was further detailed one year later by a decree stating some sectorial metrics to land use change, agribusiness, waste management and energy. In some regions such as São Paulo, there are both state and municipal level legislation. São Paulo State Climate Change Policy establishes a 20 per cent reduction target over a 2005 baseline until 2020, whereas the municipal level sets a 30 per cent reduction target over a 2005 baseline until 2012. The framework currently under design roughly addresses energy issues, but it is expected to become more specific in the short term, with sectorial measures being implemented, possibly impacting the oil and gas/mining sectors (KPMG, 2012).[17]

10. Julius, D. (1997). Globalisation and Stakeholder Conflicts: A Corporate Perspective. International Affairs (Royal Institute of International Affairs 1944-), 73(3), p.453.
11. Ruggie, J. (2004). Reconstituting the Global Public Domain – Issues, Actors, and Practices. European Journal of International Relations, 10(4), pp.499-531.
12. Johnson, E. (2003). Walking the Talk: The Business Case for Sustainable Development. Environmental Impact Assessment Review, 23(1), p.131.
13. KPMG, (2015). Global Sustainability Services — Case studies | KPMG | GLOBAL. [online] Available at: http://www.kpmg.com/global/en/services/advisory/risk-consulting/internal-audit/climate-change-sustainability-services/pages/case-studies.aspx [Accessed 7 Jan. 2015].
14. KPMG, (2015). Global Sustainability Services — Case studies | KPMG | GLOBAL. [online] Available at: http://www.kpmg.com/global/en/services/advisory/risk-consulting/internal-audit/climate-change-sustainability-services/pages/case-studies.aspx [Accessed 7 Jan. 2015].
15. Climate Change Adaptation in Rural India, (2015). ccarai.org | Home. [online] Available at: http://www.ccarai.org [Accessed 8 Jan. 2015].
16. Vial, V. (2011). Taking a stakeholders' approach to corporate social responsibility. Glob. Bus. Org. Exc., 30(6), pp.37-47.
17. KPMG, (2012). Capitalising on sustainable development in mining. 111257. NA: KPMG, p.7.

One approach taken by pioneering companies was to enter the carbon market via the Clean Development Mechanism (CDM). However, by the end of the decade many of these companies were disillusioned by the process and the uncertainty of success. Gradually, many of them abandoned the CDM and shifted to a risk management approach – comprising of GHG inventory elaboration and accounting of emissions reductions, enabling them to hedge against future regulations. Other companies adopted a wait and see policy prolonging until external stakeholders started to ask for data on their carbon footprints. The rapid interest from the investment community and organisations such as the Carbon Disclosure Project (CDP) resulted in many mining companies having to develop GHG accounting systems overnight to comply with increasing demands for non-financial information (KPMG, 2012).[18]

Conclusion

Climate change and sustainability is not just an issue for specific sectors or regions. It is a global issue that demands a systematic approach with an effective policy response. Climate change impacts is expected to accelerate with time so recognising potential adverse events, establishing appropriate risk response mechanism becomes equally important as handling business risks. Global sustainability megaforces could mean constraints, complexity and risks for business. But business leaders can do much more than simply survive the risks. With foresight and planning they can turn risks into new opportunities and pioneer actions to prepare for an uncertain future (Farrell and Hoon, 2010).[19] Organisations need to understand the vitality of the challenging risks and opportunities that it presents. At the government level the policy mechanism gives a framework that includes investments in climate change adaptation and mitigation initiatives.

India being a large and geographically diverse country, may experience every component of climate impact in the next century. Even if the impacts may not directly affect organisational performance, the ripple effects are likely to resonate throughout the value chain. With increased scrutiny by stakeholders and commitment of governments towards the acceptable phenomenon of climate change it could compel organisations to think beyond their traditional business style and focus more on handling risks via climate change and sustainability.

18. KPMG, (2012). Capitalising on sustainable development in mining. 111257. NA: KPMG, p.7.
19. Farrell, J. and Hoon, A. (2010). Whats your company's risk culture. USA: KPMG information, Press release.

Risk analytics

Abhijit Varma
Partner, IT Advisory, KPMG in India

Introduction

Risk can be alter ego of a CEO in a VUCA world where managing risk continues to be a big challenge. Traditionally, risk management used less technology and was heuristic based. As decisions and choices become more significant, there is a need to have robust risk models. Proper analysis of data helps understand key risk factors and their relative impact on the organisation with improved precision and also to identify future risks long before they become a reality. The above factors are leading more and more organisations towards risk analytics as a key part of their risk management strategies.

As per a recent joint study conducted by NASSCOM and CRISIL Global Research and Analytics, risk analytics is expected to become a USD50 billion industry globally by the year 2020[1], which could translate to a business of USD 2.5 billion for service providers in analytics from India, from a revenue of USD 700 million in FY 2013. This rise is expected to be driven by demand from financial services and corporate sectors.

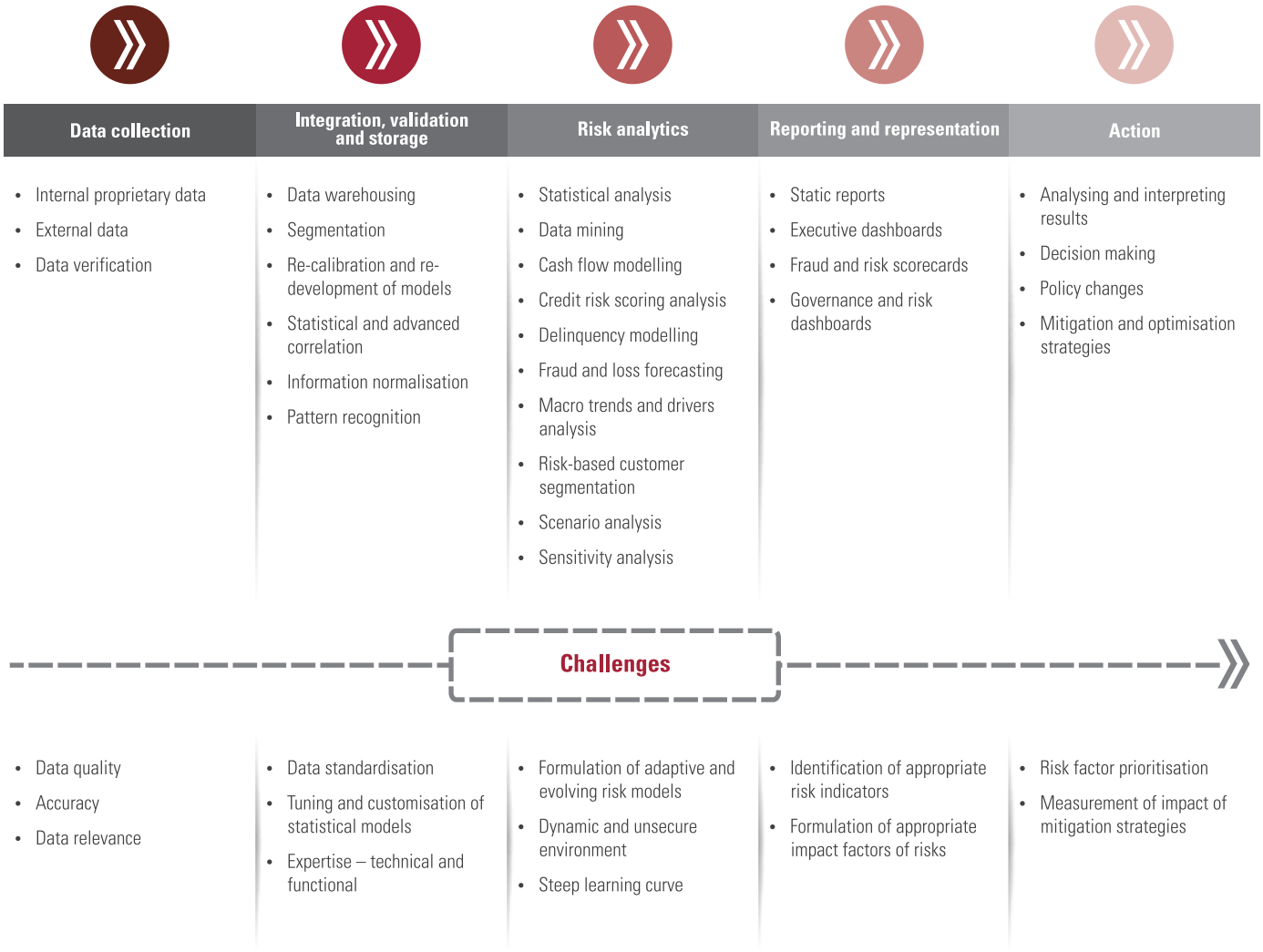
Some key applications of risk analytics are as follows:

- Enable organisations make better judgments on investment, acquisition, financial modelling, and ROI
- Help organisations meet ever increasing regulatory requirements across sectors and geographies
- Improve credit performance to better manage liquidity positions in the banking sector
- Help insurers across investment decisions, risk exposure, pricing and loss reserving
- Enable capital market firms to manage risk exposure and trading decisions
- Enable fraud detection and mitigation
- Make social media initiatives secure
- Analysis of data security threats and vulnerabilities penetrating through cyber sources.

1. Based on data published on www.informationweek.in

Risk analytics in the industry

The following diagram represents a generic value chain of a Risk Analytics framework applied in industry:



Source: CRISIL GR&A Analysis

Risk analytics technology is applied into credit risk management, fraud detection and prevention, industry benchmarking and validation, and liquidity risk analysis. The implementation helps enterprises to precisely define, understand and manage their risk profile. Risk analytics is relevant across multiple domains and is being implemented in credit risk and market risk assessment along with operational and cyber risk evaluation.

Government and healthcare verticals take the major piece of the risk analytics market pie. Other than these verticals, the market has a wide portfolio in banking, insurance, financial services, manufacturing, transportation and logistics, telecommunication and IT.

Application of risk analytics in industry is spread across horizontals and verticals as follows:

Application of risk analytics across horizontals

Strategic

- **Demand:** On-demand risk analytics, risk-based pricing
- **Customer retention:** Visual risk analytics, brand risk analytics, customer behavior analytics
- **Pricing:** Stress testing, Risk-based pricing
- **R&D:** Portfolio modelling
- **JV/Partnership:** Risk-based acquisition strategy

Operational

- **Cost Control:** Static stress testing
- **Supply chain issues:** Supply chain risk analytics, scenario analysis, stress testing
- **Employee issues like fraud:** Cyber security analytics, identity risk management, fraud/threat detection, financial crime management
- **Regulation:** Regulatory interpretation and impact assessment

Financial

- **Credit risk, liquidity and cash flow:** Liquidity risk analytics, credit risk analytics, credit risk scoring analytics, market/credit stress testing
- **Capital requirements:** Capital adequacy assessment
- **Trading:** Trading and market risk analytics
- **Audit:** Audit analytics

Environmental

- **Macroeconomic:** Systemic risk analytics, extreme event modelling, complex event processing
- **Natural disasters:** Real-time climate analytics, catastrophe risk modelling
- **Political issues:** Systemic risk analytics
- **Legal issues:** Compliance analytics

Application of risk analytics across verticals

Financial services

- Basel I&II analytics
- Asset and liability management
- Capital allocation
- Counterparty credit risk management

Insurance

- Insurance risk factor profiling
- Claims analytics and optimisation
- Actuarial risk analytics
- Leakage and predictive modelling
- Reinsurance strategy

Manufacturing

- Supplier risk analytics
- Product pricing
- Market trend analytics
- Operational safety analysis and accident prevention

Logistics and transportation

- Carrier risk analytics
- Process risk management
- Driver risk analytics and segmentation
- 3PL monitoring and evaluation

Source: CRISIL GR&A Analysis, Industry Reporting

Application and impact of the use of risk analytics in various sectors:

Financial services

The financial services sector presents a strong case for analytics in risk management as it has to operate under stringent regulatory environment. Also the focus for this sector is to develop models which are more risk-adjusted.

For instance, following is a problem faced due to Dodd-Frank regulations:

Challenge: A global financial firm needed updates on regulatory guideline/requirements of the Dodd-Frank Act and the effective dates for these changing requirements.

Solution: Developed a 'Dodd-Frank tracker' to deliver updates as well as analytics on the requirements of the Dodd-Frank Act, its various phases of implementation, and the recent developments related to the Act.

Benefits: The tracker gives client teams access to a common source for regulatory updates affecting diverse teams across the firm.

Banking

Risk analytics in the banking sector is primarily driven by factors such as growth, expansion, regulatory pressures and credit monitoring, and investments in enterprise risk and performance dashboards. Risk analytics is adopted across various functions such as risk governance, credit processing, capital management, and marketing at various stages of maturity.

Challenge: Low product profitability faced by a global consumer finance organisation.

Solution: Utilised risk analytics for multiple product lines across various geographies such as the USA, Latin America, Europe, Australia, and Asia. The methodology included models and strategies to manage risk across the product life cycle through loss mitigation, revenue enhancement, and fraud control.

Benefits: A net income impact of USD 60 million for the US portfolio due to risk analytics and savings of around USD 22 million was achieved by utilising collection strategies and operations.

Source: Risk Analytics Taking the risk out of Business by Nasscom

Insurance

The insurance sector faces risks that range from natural disasters to new forms of risks such as cyber-crime, claims fraud, patient risk of insured population, etc., Insurers are looking at risk analytics to augment business intelligence capabilities with newer techniques in modelling, claims analytics and fraud analytics.

Following are few cases from some players in the insurance sector:

A large Indian Life Insurance firm

Challenge: Implement analytics in various phases of product lifecycle management ranging from product development to product management and also product pricing accuracy evaluation.

Solution: Financial security modelling and risk evaluation

Benefits: Improved risk management by implementing a product pricing model tuned with industry risks and which is competitive in the market and provides consistent results.

A large EU Insurance firm

Challenge: Disparate legacy systems, heavy reliance on spreadsheets and multiple reporting mechanisms added to the confusion over what data is required for Solvency II legislation.

Solution: Selected SAS for its regulatory risk analytics and stress testing portfolio.

Benefits: Fulfilment of Solvency II quantitative requirements and accurate assessment of current and future risks by simulations and stress testing.

Capital markets

Persistent economic pressure and a dynamic regulatory environment are driving risk analytics in capital markets. Risk analytics is considered as means for achieving competitive advantage and an enabler for reduction in operational credit losses or market losses.

Challenge: Huge losses incurred by a U.K. based investment bank due to a dysfunctional trade model

Solution: The first step was creation of trade templates based on trading ideas and desk requirements. Then testing of models, including risk reports, scenario analysis, and performance analysis was conducted. These trade models were monitored and upgraded as and when necessary.

Benefits: The firm achieved reduction in time-to-market for new trades to upwards of 90 per cent in some cases. More than 80 trade model templates with more than USD 120 billion notional have been deployed in a year.

In addition to the aforementioned sectors, there are some key emerging areas which provide huge opportunity for adoption of risk analytics. They are listed as follows:

Mitigation of fraudulent losses

Globally, losses arising from fraudulent activities as well as data breaches are growing at an alarming rate. Organisations face various threats in terms of internal and external fraud ranging from cyber-crime, information theft to management conflict of interest and money laundering. There are several risk analytics services used for mitigation of fraudulent losses such as cyber security analytics and identity risk analytics. Upcoming services such as anti-money laundering analytics and audit analytics present opportunities to mitigate fraudulent losses proactively.

Security of social media initiatives

Social media is among the most potent risks posed by organisations globally due to the huge volume of unstructured data generated. The growing use of social media poses risks such as abuse of intellectual property, damage to brand/ reputation, etc., Numerous services have evolved in the risk analytics space to handle and mitigate these 'digital risks'. Some of them are:

- **Visual risk analytics:** Holds huge amounts of data, identifies risk patterns and presents them in a user friendly format
- **Brand risk analytics:** Scans data across social media to identify, prioritise and report emerging threats as well as people and process frameworks to help organisations respond to brand risks effectively.
- **Self-service risk analytics:** Enables the various levels of businesses to access data from social media through ad-hoc queries and custom reports.
- **Next generation risk analytics:** Includes real-time analytics and model calibration, data aggregation at multiple levels, pre-trade analysis and a variety of other tools for mitigating risks on a continuous basis.

Tools

Risk analytics basically uses mathematical methods and tools to address a broad range of risk-related activities performed by an organisation. The risk analytics market offers varied tools such as risk calculation engines, scorecards and visualisation tools, extract, transform and load software, dashboard analytics and risk reporting. Its integration with real-time analytics tools has led the market to make informed decisions based on the most relevant data set, the real time data, rather than outdated and irrelevant historical data.

In this section, we look at various tools employed for the use of risk analytics. Some popular risk analytics tools offerings in various sectors are as follows:

Finance sector	Operational risk	Fraud management	Enterprise risk analytics
Oracle Financial Services Operational Risk Analytics	Oracle Primavera Risk Analysis - Life Cycle Analytics	SAP Fraud Management	Moody's Analytics Enterprise Risk Solutions
SAP Enterprise Risk Reporting for Banking	IBM Operational Risk Management	Accertify Interceptas	Teradata Enterprise Risk Management Solutions
SAP HANA Finance and Risk Analytics for Banking		FICO Falcon Fraud Manager	Angoss predictive analytics for risk management
IBM AlgoRisk		GDS Dataview 360	MongoDB
			Bringa Risk Analytics

Finance sector

Regulatory oversight and increasingly complex asset classes are revolutionising risk management, compliance, security and data management in today's financial services industry. Financial institutions need real time analytics to read the dynamic market fluctuations and assess their potential impacts and threats as well as evaluate the factors holistically across the enterprise, to mitigate risk, improve profitability and comply with regulatory requirements.

Operational risk

Evaluation of factors of loss which result from inadequate operational processes or losses triggered by external events can be defined as operational risk analytics. This analytics can span over the systems as well as people. Operational risk management has become one major part of enterprise risk management strategies for organisations from various sectors. Operational risk management involves application of risk analytics to various business decisions and projects.

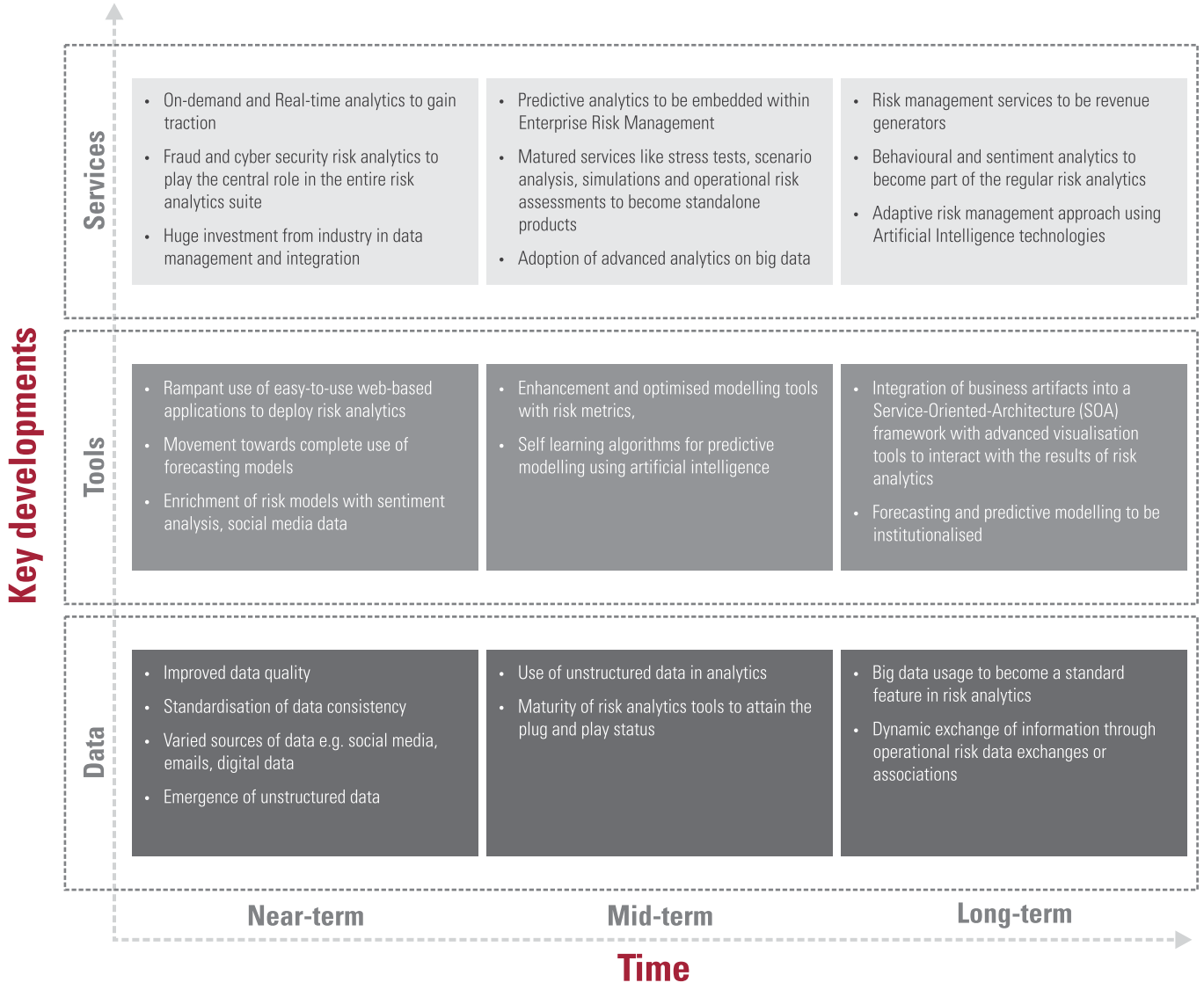
Fraud management

Fraud management involves pre-emptive fraud detection and decision management based on managed risk services.

Enterprise risk analytics

Enterprise Risk Analytics encompasses risk management approach for the whole enterprise, based on their required analytics maturity level and industry.

The following diagram illustrates the key trends in risk analytics.



Source: CRISIL GR&A Analysis, Industry Reporting

Points to ponder

As organisations begin to adopt a holistic view on risk assessment, risk analytics is increasingly being used across business units and functions. This cross functional use of risk assessment provides an organisation the platform to react to the risk factors quickly and incorporate new risk enquiries. The next suite of applications within risk assessment is expected to be based on predictive modelling as compared to the evaluative and diagnostic techniques currently being used.

Areas within risk analytics that are pegged to gain momentum include:

- On-demand risk analytics
- Cyber security risk analytics
- Audit analytics
- Social media analytics.

Business continuity planning : Need of the hour for India Inc.

Kunal Pande
Partner, IT Advisory, KPMG in India

> "You cannot escape the responsibility of tomorrow by evading it today."
>
> **- Abraham Lincoln**

In a span of a few odd years, many enterprises around the globe have grown exponentially by leveraging globalisation and its network effects to achieve competitive advantages on a scale hitherto unseen. However, natural and man-made disasters have been increasingly impacting the continuous growth of these enterprises. In 2013, approximately 158 man-made and 150 natural catastrophes occurred. Almost 26,000 people either lost their lives or went missing in these disasters and the total economic losses were about USD140 billion[1]. 2014 was also marked by very unlikely tragedies - aircrafts of Air Asia and Malaysian Airlines, respectively, went missing. The losses were immeasurable - not just financial and reputational but even loss of life. Enterprises today are required to understand the strength of Business Continuity Planning and Disaster Recovery Planning to handle such difficult times and maintain a competitive edge.

India has also not been spared from these disasters. The year 2004 witnessed tsunami in the coastal regions of Tamil Nadu and four other states which purloined more than INR3000 crore from the Indian economy. Countless people lost lives. ONGC had to shut down its operations in three oil producing wells for three days to assess the damage. A number of hotels had to suspend business due heavy damages. Losses to the shipping industry were estimated at around INR200 crore due to the loss of four ships. The Asian economy suffered losses of more than USD13.6 billion as multiple countries were affected due to the disaster. Similarly the dreadful 26/11 terrorist attack led to loss of lives, property, revenue. The share price of The Indian Hotels Company Limited fell to as low as INR40.20 which was an all time low; the insurance sector took a whopping INR400 crores hit. The tourism industry and overseas investment saw a major downfall. The total financial losses due to the attack were estimated to be around USD800 million[2].

Not just disasters, the overall weakness in the Indian infrastructure is apparent, where one heavy downpour leads to massive delays in public transport or one state overdrawing power results in a cascading collapse of the entire regional power grid. India has witnessed a number of disasters where a large section of market and economy has been impacted. One cannot forget the flash floods in Mumbai in 2005 which were aggravated due to lack of effective sewerage infrastructure. Such disasters undoubtedly severely impact the reputation of a growing economy like ours.

1. http://reliefweb.int/report/world/sigma-no-12014-natural-catastrophes-and-man-made-disasters-2013-large-losses-floods-and
2. www.ficci.com/Sedocument/20228/India-Risk-Survey-2013.pdf

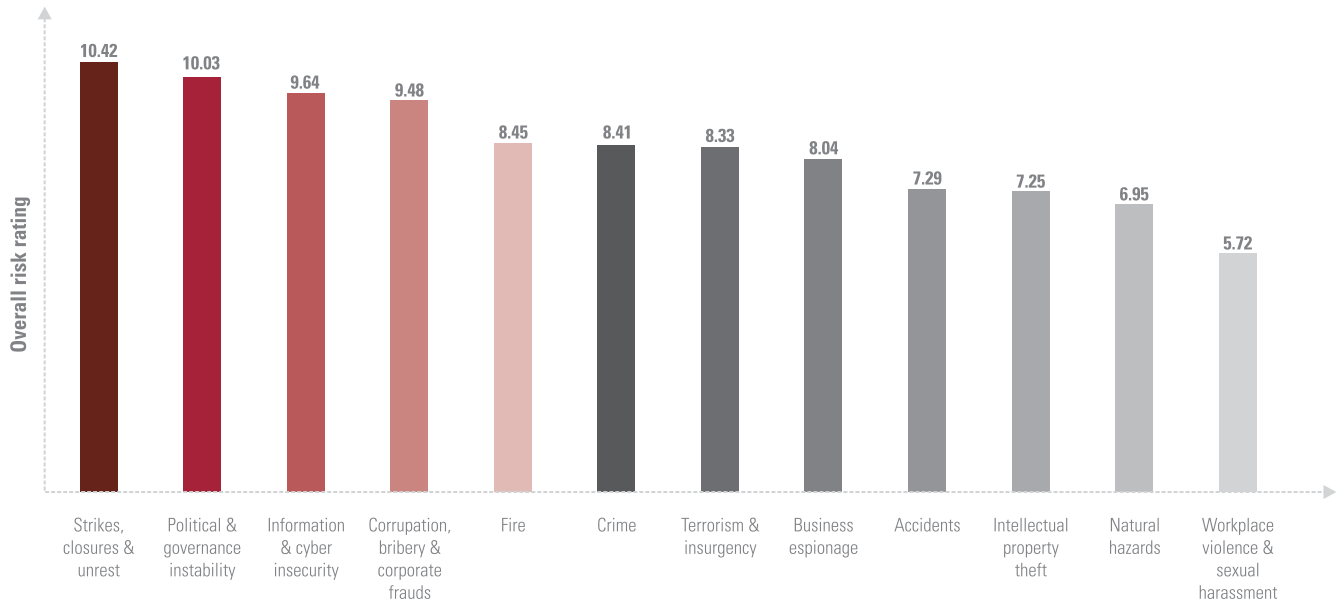
The Indian market which is riding the crest of a change of government and the resulting optimism, is witnessing growth and business transformations, and is cautiously en-route towards becoming a center for both domestic and foreign investments. An environment of better infrastructure, pool of talented resources, large local markets and ease of investment would be icing on the cake. With the government's push on 'Make in India', Indian enterprises are poised to play a significant role in the global supply chain. As a result, disruption of operations in Indian enterprises may actually result in the disruption of business for their customers as well as suppliers. Indian corporates, being more integrated into the global supply chain, thus need to incorporate business continuity as a part of their growth strategy rather than only for operational risk management.

Further, thanks to technology and other concomitant aspects of globalisation, and shifting of the economic landscape from west to east, corporates in the west and east alike have spread their businesses across continents. As a result, the decisions taken in one part of the organisation may have an impact several thousand nautical miles away. The interconnected world marked by massive global investments that are inextricably tightening economic interdependencies across regions, raises a number of questions. Have these corporates truly considered their risk exposures vis-à-vis operations, markets and regulations? Is their rapid growth backed by a robust and resilient plan to combat the occurrence of any unplanned event? Have they performed detailed due diligence before making investments? Are they ready to show a commendable and positive growth even in the times of disruption? Under-preparedness shall leave corporates significantly exposed to risk factors wihch may even destabilise economies. While the role of the state and international community in creating a robust business ecosystem cannot be emphasised more, until the overall ecosystem evolves, individual businesses will have to 'fend for themselves' to sustain their and their customers' business operations by putting in place robust Business Continuity measures.

> "Business continuity is not a project with a beginning and an end date, it is a programme to be managed indefinitely."
>
> **- Business Continuity Management[3]**

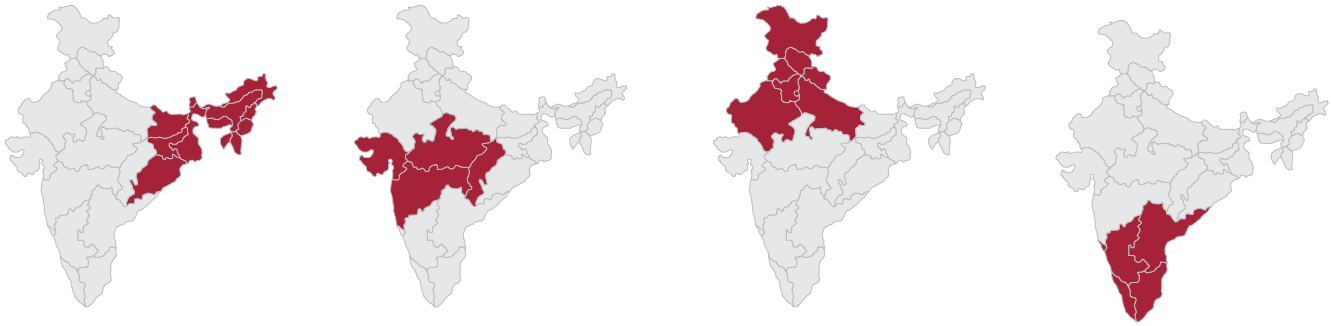
A survey by Pinkerton and Federation of Indian Chambers of Commerce and Industry (FICCI) ranks the risks in a typical Indian market scenario for the year 2013 which has highlighted strikes closures and unrest as the biggest risk to the Indian enterprises, followed by political and governance instability.

High profile cases such as Target, Sony Pictures, and ElectraCard have led to Cyber Threat gain prominence as a cause for disaster. World over governments have taken steps to address this threat; Government of India has set up NCIIPC as the nodal agency for establishing policies and practices, providing guidance and build preparedness for Cyber Security. The Pinkerton survey results also indicate a rise in ranking for information and cyber insecurity.



Source: India Risk Survey-2013 – FICCI

3. www.ficci.com/Sedocument/20228/India-Risk-Survey-2013.pdf



East

- Political and governance instability
- Strikes, closures and unrest
- Terrorism and insurgency

West

- Political and governance instability
- Terrorism and insurgency
- Strikes, closures and unrest

North

- Strikes, closures and unrest
- Political and governance instability
- Corruption, bribery and corporate frauds

South

- Strikes, closures and unrest
- Information and cyber insecurity
- Political and governance instability

Source: ndia Risk Survey-2013 – FICCI

While, the survey results highlight a number of threats, it is vital that corporates understand that the risks each of them face could be different depending on business complexities, regional subtleties and technological challenges. Corporates should perform a similar assessment, understand risks they are exposed to and build effective business continuity capabilities.

> "Not everything that counts can be counted, and not everything that can be counted counts"
>
> **–Albert Einstein**

BCP from the regulators perspective

For financial institutions regulators in India have published guidelines on business continuity and disaster recovery. The Securities and Exchange Board of India (SEBI) has come up with a circular for implementing BCP and disaster recovery plans to ensure smooth business functioning with minimal downtime in the event of a disaster[4].

The Reserve Bank of India's (RBI) circular on Operations Risk Management stresses on the importance of a BCP and makes the Board of Directors of Banks as the owners of the plan. The circular also lays down the need for the banks to disclose information relating to major failures of critical systems and the steps taken to avoid such failures in future. An annual review and update of a bank's BCP plan and any underlying third party service provider's BCP plan is mandatory as part of the circular[5].

The Insurance Regulatory and Development Authority (IRDA) has also laid down its guidelines for insurers to perform a due diligence around the business continuity plans in case the services are outsourced to a third party[6].

Telecom Regulatory Authority of India (TRAI) has been publishing several consultation papers and guidelines for the telecom operators to provide a supervision on their operations at the time of crisis or disasters[7].

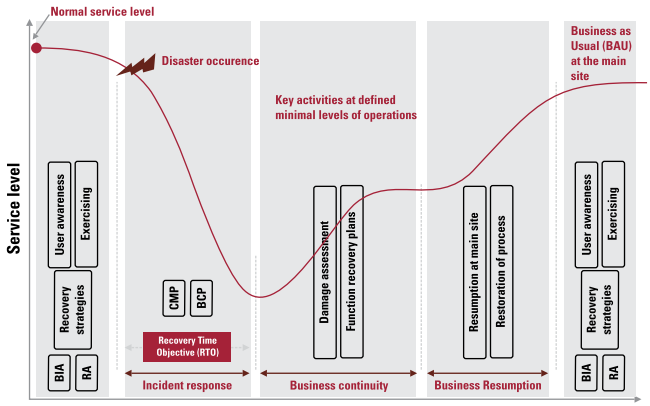
The International Standards Organization (ISO) has defined ISO 22301 standard to implement Business Continuity and Disaster Recovery capabilities for organizations. In the financial services sector the Basel Committee established the Basel II framework that also focuses onbusiness continuity. The framework identifies broad types of operational risk, including continuity risk, such as damage to physical assets, system failures, events that have the potential to result in substantial losses, which can ultimately lead to not only business disruption but in extreme cases to organisations going out of business. It requires all banks to put BCP/ DR plans in place to ensure continuous operations and limit losses. The publication on 'High Level Principles of Business Continuity' provides seven guiding principles for effective BCM and ingeminates that BCM is a vital component of Operational Risk Management (ORM)[8].

5. www.sebi.gov.in/cms/sebi_data/attachdocs/1334316648611.pdf
6. http://rbi.org.in/Scripts/NotificationUser.aspx?Mode=0&Id=2205
7. https://www.irda.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo954
8. http://webcache.googleusercontent.com/search?q=cache:p6RfADVJMx0J:www.geminare.com/pdf/U.S._Regulatory_Compliance_Overview.pdf+&cd=1&hl=en&ct=clnk&gl=i
9. http://www.continuityinsights.com/articles/2004/12/basel-ii-and-business-continuity

World over governments and regulators have laid down regulations and rules for business continuity. For example, Health Insurance Portability and Accountability (HIPAA) act mandates all health related organisations to have a documented and approved data back-up plan, disaster recovery and emergency plans. National institute of Standards and Technology (NIST) have issued multiple publications concerning security controls with specific requirements around continuity planning and testing and BCP/ DR and continuity of operations plan.

Traditional and emerging BCP practices

Business Continuity Management (BCM) is defined by the Business Continuity Institute (BCI), UK as a 'holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities'. The diagram below depicts the elapsed time between the crisis striking a business operations and resuming of normal business operations. The aim should be to reduce this time as much as possible.



Source: KPMG in India

The business environment is changing rapidly and moving towards a real-time 24*7 operations model. The need of undisrupted connectivity and continuous information has made the environment more complex. Enterprises are required to stay updated with the latest technologies and be aware of the latest trends to combat the challenges faced by the ever changing business environment and regulatory norms. In an increasingly digital world, with rise in connected devices (mobiles to industrial equipment) - there is a need to adopt technologies that enable high-availability systems, real-time communications and faster recovery times while minimising cost[9]. Disruption in such a world could mean deprivation of vital resources to people at large.

Enterprises today can take advantage of advances in telecommunications, information technology, data storage solutions, mobile devices, social media, virtualised environments, and cloud computing to increase resiliency and data storage capabilities[10]. While the business continuity plan will differ from enterprise to enterprise due to differences in underlying business risks, enterprises can leverage technology to adopt low-cost approaches for efficient continuity. Implementation of Virtual Desktop Infrastructure (VDI), for example, can ensure access to the critical systems by the employees at the time of a disaster with a minimal cost. These not only reduce productivity losses but also prevent reputational losses as well.

Technology can also enable continuity processes directly. For e.g. Log analysis software available in the market today can help assess the impact of the events on a real-time basis. This coupled with in-built reporting and add-on analytics tools can improve the effectiveness of the continuity planning. Introduction of automated tools to develop the crisis management plans based on the risks identified have simplified the overall process of BCM. Backup as a Service (BaaS), Storage as a Service (STaaS), Disaster Recovery or Replication as a Service (DRaaS), and Software as a Service (SaaS) are few of the Cloud based services which are picking up pace and have great potential in the coming days. While the operating cost of using Cloud services may be higher than Capex on IT, they provide a pay-per-use model along with being more resilient to location specific disasters.

Effective communication is also one of the vital requirements in effective management of a crisis. Automated call trees can be implemented which updates information from the HR databases to determine efficient and timely communication. While BCP and DR plans have been existing for a relatively long time now, the inclusion of mobile devices, and social media at the enterprise level have given it a new direction.

However, new technology also brings new challenges for organisations to manage: for example, several organisations are required to understand the nuances of social media and ensure that right information is communicated at the time of crisis as any confusion can lead to a failure of the BCP/ DR plan. Failure to do this can result in public relations challenges. For example, when a Boeing 777 flying from Seoul, South Korea crashed at San Francisco International Airport on landing in July 2013, an observer waiting to board another flight snapped a photograph of the accident with her mobile phone and uploaded it on Twitter less than one minute after the impact[11]. Within 30 minutes, there had been more than 44,000 tweets about the accident. Such incidents reiterate that if the organisation does not use social media with agility and speed, it may often lose the opportunity to provide factual information and influence the developing narrative.

9. http://webcache.googleusercontent.com/search?q=cache:l-zCl-k3wmIJ:www.infosecurityeurope.com/__novadocuments/48836%3Fv%3D635307737294830000+&cd=1&hl=en&ct=clnk&gl=in
10. http://webcache.googleusercontent.com/search?q=cache:l-zCl-k3wmIJ:www.infosecurityeurope.com/__novadocuments/48836%3Fv%3D635307737294830000+&cd=1&hl=en&ct=clnk&gl=in
11. http://jalopnik.com/twitter-user-accidentally-captures-image-of-boeing-777-687945526

Case in point: Business continuity initiative for a retail chain

A large Indian retail chain with stores in two distinct formats – Hypermarkets (HM) in Metros and Tier I cities and Supermarkets (SM) in Tier II and Tier III towns was facing challenges in sustaining profitability of its operations due to a constant stream of local disruptions faced by individual stores. Adding to local challenges were teething troubles of a weak IT infrastructure given that some stores operated out of remote locations. A need was felt for a Business Continuity Management Framework (BCMF) for the network of stores and offices.

Multiple formats, wide geographical spread across the country, complex supply chain management, presence of warehouses at remote locations making it non accessible in time of need, poor IT Infrastructure were some of the key challenges that lead to the need of having a Business Continuity Plan in place. The challenge of developing a BCMF for a large network spanning across hundreds of SMs and tens of HMs was resolved by selecting representative samples of a Zonal Office, Hypermarket, Supermarket, Warehouses and repacking facilities in addition to the Head Office.

The entire project spanned over a period of six months for sampled locations. The approach was to identify mission critical activities performed, analyse possible disaster threats and resulting outage scenarios, and devise strategy to resume business operations in an outage scenario. In order to ensure that the BCP highlights the procedures to be followed in the event of an outage at any location, processes at various departments for sampled locations were understood, critical infrastructure and IT applications identified and any interdependencies for processes were also identified.

All the identified processes were studied and classified based on the impact to the location if they were to be unavailable. Data gathered during the understanding phase was used to perform a Business Impact Assessment to determine the Minimum Tolerable Time of Disruption (MTTD) and Recovery Time Objective (RTO) for each process.

This information in conjunction with information on critical infrastructure, IT applications and interdependencies was used to arrive at requirements for IT Disaster Recovery, repair/ replacement/ sourcing arrangements for critical infrastructure and any alternate arrangements for critical staff members.

Some innovative methods identified for continuity of operations included use of VDI by the key staff members to enable anywhere access to critical data, providing staff at Zonal offices with mobile computing devices, cross training of Warehouse staff to operate Hyper and Supermarkets (and vice versa) and cross allocation of staff between various stores within the vicinity of each other to enable sharing of staff by stores in the event of disaster. In addition each location was subject to a risk profiling exercise to access the impact of various threats on the location. This information was used to develop a customised Crisis Management Plan (CMP) in addition to the Business Continuity and Disaster Recovery plans.

Conclusion

The world is undergoing an unprecedented social, cultural and technological transformation which has resulted in emergence of several man-made risks such as social unrest, adding to the long list of the natural disasters.

Business Continuity Management has become an essential component to run any organisation to ensure that the client requirements are met even in the event of a disruption. By adopting a robust business continuity management processes, India Inc. can not only gain a competitive edge with the existing market players but can also attract new business. A robust Business Continuity plan acts as a shield to protect organisation's brand and reputation. An organisation can focus on the following points while implementing their BCP:

1. Organisations must integrate BCM into enterprise strategic planning to meet market demands and regulatory requirements. The need of the hour is to understand that continuity is not for the few departments or head office only.
2. Business continuity, similar to other strategic drivers of the organisation, needs to have robust governance processes to enforce accountability within the organisation and to ensure management focus on evolving needs of continuity. Continuous assessment, update, and communication of the BCP can keep the organisations ready for the worst and synchronised with the emerging trends.
3. Effective implementation of Business Continuity requires clarity in scope definition which shall help ensure inclusion of the critical business process, their dependencies and a holistic approach covering people, process, technology and infrastructure.
4. Technology enabled strategies for managing business continuity can be both cost efficient and reliable than traditional approaches. This requires a technology aware and innovative approach to be taken by the management.
5. Media and people management at the time of crisis is a key element of Business continuity in today's times. Social media management is an emerging area of business continuity and crisis management.

> "Better to have a Business Continuity plan and not need it, than to need the plan and not have it.[12]"

12. www.continuitycentral.com/quotes,author.pdf

About **CII**

The Confederation of Indian Industry (CII) works to create and sustain an environment conducive to the development of India, partnering industry, Government, and civil society, through advisory and consultative processes.

CII is a non-government, not-for-profit, industry-led and industry-managed organisation, playing a proactive role in India's development process. Founded in 1895, India's premier business association has over 7200 members, from the private as well as public sectors, including SMEs and MNCs, and an indirect membership of over 100,000 enterprises from around 242 national and regional sectoral industry bodies.

CII charts change by working closely with Government on policy issues, interfacing with thought leaders, and enhancing efficiency, competitiveness and business opportunities for industry through a range of specialised services and strategic global linkages. It also provides a platform for consensus-building and networking on key issues.

Extending its agenda beyond business, CII assists industry to identify and execute corporate citizenship programmes. Partnerships with civil society organisations carry forward corporate initiatives for integrated and inclusive development across diverse domains including affirmative action, healthcare, education, livelihood, diversity management, skill development, empowerment of women, and water, to name a few.

The CII theme of 'Accelerating Growth, Creating Employment' for 2014-15 aims to strengthen a growth process that meets the aspirations of today's India. During the year, CII will specially focus on economic growth, education, skill development, manufacturing, investments, ease of doing business, export competitiveness, legal and regulatory architecture, labour law reforms and entrepreneurship as growth enablers.

With 64 offices, including 9 Centres of Excellence, in India, and 7 overseas offices in Australia, China, Egypt, France, Singapore, UK, and USA, as well as institutional partnerships with 312 counterpart organisations in 106 countries, CII serves as a reference point for Indian industry and the international business community.

Confederation of Indian Industry (CII)
The Mantosh Sondhi Centre
23, Institutional Area, Lodi Road, New Delhi – 110 003 (India)
T: 91 11 45771000/24629994-7 • F: 91 11 24626149
E: info@cii.in • W: www.cii.in

About **KPMG**

KPMG in India

KPMG in India, a professional services firm, is the Indian member firm of KPMG International and was established in September 1993. Our professionals leverage the global network of firms, providing detailed knowledge of local laws, regulations, markets and competition. KPMG in India provide services to over 4,500 international and national clients, in India. KPMG has offices across India in Delhi, Chandigarh, Ahmedabad, Mumbai, Pune, Chennai, Bangalore, Kochi, Hyderabad and Kolkata. The Indian firm has access to more than 8,000 Indian and expatriate professionals, many of whom are internationally trained. We strive to provide rapid, performance-based, industry-focussed and technology-enabled services, which reflect a shared knowledge of global and local industries and our experience of the Indian business environment.

KPMG International

KPMG is a global network of professional firms providing Audit, Tax and Advisory services. We operate in 155 countries and have more than 162,000 people working in member firms around the world.

The KPMG Audit practice endeavours to provide robust and risk based audit services that address member firms' clients' strategic priorities and business processes.

KPMG's Tax services are designed to reflect the unique needs and objectives of each client, whether firms are dealing with the tax aspects of a cross-border acquisition or developing and helping to implement a global transfer pricing strategy. In practical terms that means, KPMG firms work with their clients to assist them in achieving effective tax compliance and managing tax risks, while helping to control costs.

KPMG Advisory professionals provide advice and assistance to help enable companies, intermediaries and public sector bodies to mitigate risk, improve performance, and create value. KPMG firms provide a wide range of Risk Consulting, Management Consulting and Transactions and Restructuring services that can help their clients respond to immediate needs as well as put in place the strategies for the longer term.

Acknowledgement

The report would not have been possible without the commitment and contribution of the following individuals:

KPMG Report Development and Review Team

Abhijit Varma, Arjun Rattan, Atul Gupta, Disha Agarwal, Divya Mishra, Jignesh Desai, Jignesh Oza, Jiten Ganatra, Kaushal Desai, Kunal Pande, Manish Kumar, Manpreet Singh, N Subramanian, Nikhil Kulkarni, Nisheeth Srivastava, Prashant Bhat, Rashmi Rani, Remedios Dsilva, Rajesh Patel, Ruchira Dabas, Santosh Jayaram, Sandeep Gupta, Subashini Rajagopalan.

KPMG in India contacts:

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

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

Akhilesh Tuteja
Head
IT Advisory
T: +91 124 307 4800
E: atuteja@kpmg.com

The Confederation of Indian Industry (CII) contact:

Suresh Senapaty
Chairman, CII National Risk Summit 2015
Executive Director and
Chief Finance Officer, Wipro Limited
Confederation of Indian Industry
T: 91 80 4204 4097 / 98

kpmg.com/in

Latest insights and updates are now available on the KPMG India app.
Scan the QR code below to download the app on your smart device.

Google Play | **App Store**

Printed in India. (THL0115_017)