India Insights

The Indian economy newsletter

April 2018

In this issue

India at a glance
Quarterly update Q3FY17-18

Tune in
Potential impact of National Health Protection Scheme (NHPS) on the overall healthcare sector – opportunities and implementation challenges ahead

Spotlight
Comprehending the threats of data leakage and preserving Unpublished Price Sensitive Information (UPSI)

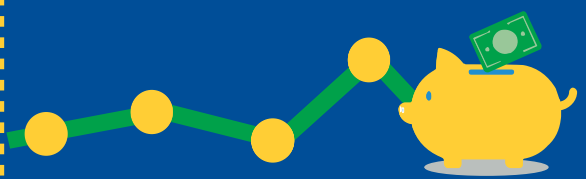
Opinion
Cyber preparedness can propel your business towards new avenues of revenue growth

India at a glance: Quarterly update

Q3FY17-18 (October-December 2017)

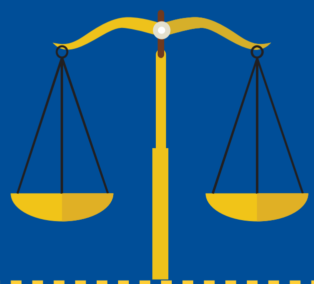
Macro economy[1]

- **Gross Domestic Product (GDP) expanded at 7.2 per cent in Q3FY17-18 vis-à-vis 6.8 per cent in Q3FY16-17**
  - Growth was backed by a rebound in industrial activity, especially manufacturing, construction and an expansion in agriculture activity (compared to the previous quarter)
  - Supply shocks induced by demonetisation and Goods and Services Tax (GST) have eased down considerably
  - A sharp pick-up in investment; 12 per cent rise in Gross Fixed Capital Formation (GFCF)
  - Manufacturing has benefited in the third quarter from the restocking exercise post the implementation of GST and demonetisation.



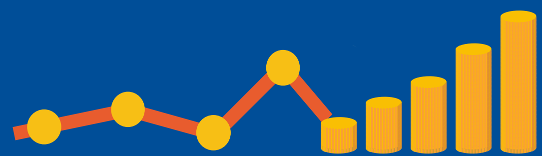
Government finance[2]

- India's fiscal deficit stood at 113.6 per cent (of the budgetary target for FY17-18) for the period April-December 2017 on account of GST implementation and deferment of telecom spectrum auction
- India's trade balance worsened and stood at its widest at USD14.88 billion in December 2017 vis-à-vis – USD10.54 billion in December 2016.



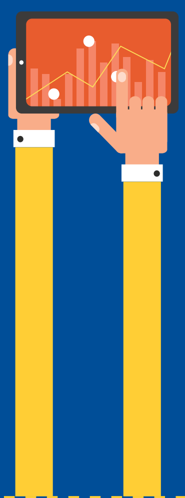
Inflation[3]

- India's retail inflation measured by the Consumer Price Index (CPI) stood at 5.21 per cent in the month of December 2017 - up from 4.88 per cent in November 2017 and 3.41 per cent in December 2016
- The annual rate of inflation measured by the Wholesale Price Index (WPI) stood at 3.58 per cent (provisional) for the month of December 2017 over December 2016 (2.10 per cent), lower than (provisional) 4.02 per cent for the previous month[4].



Foreign Direct Investment[5]

- India received Foreign Direct Investment (FDI) worth USD35.94 billion during April-December 2017 vis-à-vis USD35.84 billion during the same period last year, a rise of 0.27 per cent from last year.



Forex[6]

- Foreign exchange reserves stood at USD404.92 billion as on 22 December 2017, aided by an increase in foreign currency assets.

1. Press Note on Second Advance Estimates of National Income 2017-18 and Quarterly Estimates of Gross Domestic Product For the Third Quarter (Q3) of 2017-18; MOSPI, 28 February 2018
2. Key Economic Indicators; Office of Chief Economic Advisor, DIPP; updated as on 20 February 2018
3. All India Inflation rates (%) based on Consumer Price Index (CPI) and Consumer Food Price Inflation (CFPI) on Base 2012=100; CSO; Office of Chief Economic Advisor; Updated as on 7 March 2018
4. Index Numbers of Wholesale Price in India (Base: 2011-12 = 100), Review for the month of December, 2017
5. Quarterly Fact Sheet, Fact Sheet on Foreign Direct Investment (FDI); updated up to December, 2017
6. Weekly Statistical Summary, Reserve Bank of India, 22 December 2017

Tune in

Potential impact of National Health Protection Scheme (NHPS) on the overall healthcare sector – opportunities and implementation challenges ahead

As envisioned under the National Health Policy, 2017, the Union Budget 2018–19 has taken a long stride towards Universal Health Coverage (UHC), with a focus to increase the health coverage for the under-privileged and the bottom-of-the-pyramid sections of the society. Under the Ayushman Bharat programme, the government has announced measures to holistically cover primary, secondary and tertiary healthcare services. This being said, the NHPS will cover 10 crore (100 million) families with an annual coverage of INR5 lakh (approx. USD7685) per family. The scheme is expected to boost demand for medical services in the country and provide an opportunity to healthcare providers and insurance companies to partner with the government. It may also reduce the Out Of Pocket (OOP) expenses on healthcare, leading to increased disposable incomes in the long run. The proposals also include an allocation of INR1200 crore (approx. USD0.18 billion) for setting up 1.5 lakh health and wellness centres under the programme, which provide comprehensive healthcare, including for non-communicable diseases[1]. The allocation of INR600 crore (approx. USD 0.09 billion) in the healthcare budget to provide nutritional support for tuberculosis patients at INR500 (approx. USD7.69) per month during the treatment period is an effort towards mitigating the financial burden of the disease and providing quality care[2].

The NHPS has paved the way for UHC in the country but the challenge lies in its implementation

Overall, the proposed measures of the budget are expected to provide an immense boost to the healthcare industry and allied services in the country. However, for the success of the initiative, a structured approach and implementation remains key. Considering the coverage of the scheme, there is a need to focus on four key areas, which would pose implementation challenges and at the same time provide opportunities to the healthcare industry.

- **Building digital infrastructure:** Coping with the massive volumes of data on citizens, records and payments calls for a robust digital infrastructure. There is a huge variation in technical capabilities across India's many states, and the IT aspects of NHPS will have to be managed carefully. In order to ease the implementation, it becomes essential to encourage the healthcare workforce to adopt technology and move towards digitisation.
- **Enrollment and reimbursements of beneficiaries:** With the ambitious aim of covering 10 crore (100 million) families under the scheme, it is essential to develop a comprehensive mechanism of enrollment of beneficiaries and build a robust project management unit.

Nilaya Varma

Partner and Head
Healthcare and Government
KPMG in India

1. Healthcare experts welcome Union Budget 2018, Pharmabiz, February 2018
2. Union Budget 2018-19, Our Point of View, KPMG, 2018

This would expedite enrollments as well as reimbursements and streamline the workflow.

– **Understanding successful global healthcare financing models and imbibing key learnings:** In choosing what will and won't be reimbursed, the NHPS could make strategic yet controversial decisions that affect almost 500 million citizens. The only response to this is to rely on transparency and evidence. A good example of this is the UK's value-for-money agency -The National Institute for Health and Care Excellence (NICE), which determines what drugs and procedures will be funded by the taxpayer based on clear thresholds of costs and benefits.

– **Patient awareness on healthcare insurance and utilisation of the services** would also play a crucial role in achieving the ultimate objective of extensive healthcare coverage in the country.

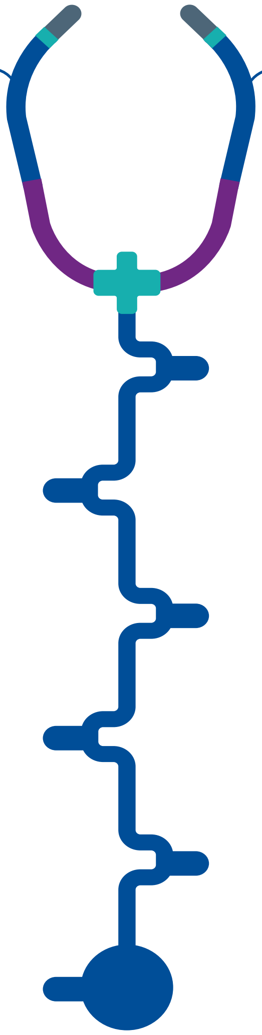
For the implementation of such a scheme, the complexity lies in scouting and devising solutions in key areas. These include preparing a model of the healthcare system financing, outlining the role of private health insurers, regulating the system and governance, charting out the components of benefit packages, developing methods of effective gatekeeping, and organising provisions to monitor and manage care.

The way ahead

The NHPS must be carefully designed to ensure that it can competently plan and purchase care for nearly 50 crore (500 million) people. To accomplish this goal, there is a need to devise an execution plan, with each step being meticulously designed, covering all the risks attached while delivering the best healthcare outcomes. The four key steps, which can potentially lead the way to the desired outcome of the scheme are:

Working on the functional building blocks of NHPS

- **Executive management functions,** including overall strategy, policy and planning; guidelines development, communication; and legal.
- **Benefits management functions,** including actuarial, beneficiary and benefits package management, and citizen rights.
- **Provider network management functions,** including compliance and quality assurance/improvement; contract management and negotiation; wellness and population health management; and infrastructure.
- **Intelligence and information functions,** including data and analytics; data security, counter-fraud; coding and IT platform management.
- **Financial management functions,** including workforce planning, organisational development and HR administration.



Developing NHPS Target Operating Model and deciding the Centre-state split

It is important to create a Target Operating Model (TOM) for the overall NHPS administrative agency. There are three important stages to this process:

- Defining NHPS's scope of operations.
- Defining the federal state split- i.e. what NHPS functions will be the responsibility of state governments, and what will controlled by the Centre.
- Defining the internal TOM for the national agency governing NHPS.

Building key capabilities and skills for NHPS

This includes laying out the organisational architecture to define the specific roles that will be needed in the start-up and steady periods, and how these will be staffed.

Setting detailed operational policies and procedures

This includes defining the roles and responsibilities of NHPS in relation to all other relevant agencies at the federal and state levels.

Spotlight

Comprehending the threats of data leakage and preserving Unpublished Price Sensitive Information (UPSI)

With a slew of economic reforms over the last four years, India has witnessed a significant rise in investor confidence. This has brought about higher investments and increased trading across listed companies in India. However, the overall buoyancy has come with its own share of detrimental costs. Companies in general, and Indian companies in particular, are exposed to new kinds of risks.

With disruptive technology advancements, data has become extremely fluid, and is often in transit through various applications, making its access much easier. On the other hand, this has opened up new channels through which perpetrators or insiders can get access to a company's confidential data or UPSI. Companies must, therefore, account for and have policies in place to manage risk emanating from the leakage of UPSI. The perils of unfair practices such as these may not only lead to a loss of investor confidence in the securities market but will eventually make it difficult for companies to raise future capital.

Mohit Bahl

Partner and Head
Forensic Services
KPMG in India

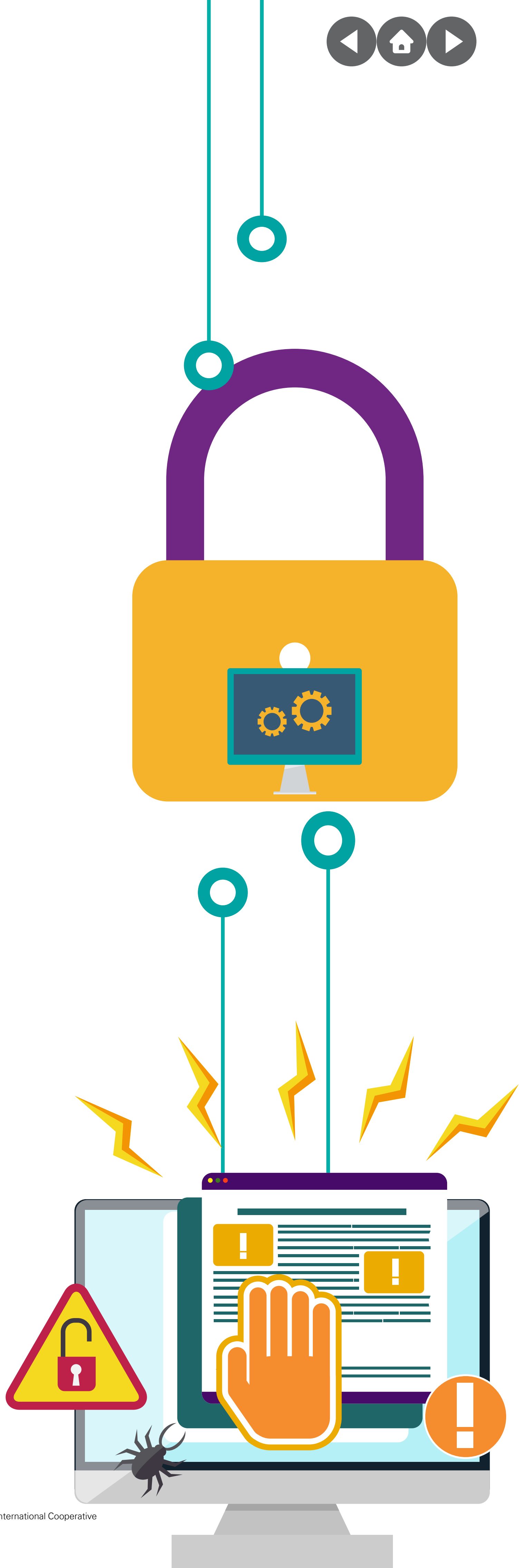
Defining UPSI[1]

UPSI typically consists of information which is confidential or not in the public domain, which when disclosed to the public is likely to materially impact the performance of a company's stock.

Usually, multiple teams are involved in handling data from various sources to create and manage datasets required for the preparation of accounts and financial statements. Some or all of these datasets are available with designated persons only.

Given this situation, companies have the prerogative and responsibility to prepare and maintain a list of designated persons and regularly update it, while also ensuring proper procedures to monitor that their trades are in place.

Further, regulations such as the SEBI (PIT) Regulations, 2015 are enforced, which prohibit insiders from communicating UPSI or trading



1. The 'insider' threat – Safeguarding UPSI, KPMG in India, 9 March 2018

Indicative lists of teams who handle UPSI

Information technology

- Financial planning and analysis
- Corporate secretarial team
- MD/CEO/ CFO office
- Audit committee
- Corporate finance and accounts
- Investor relations
- Taxation
- Board of directors
- Statutory auditors/Tax consultants

in securities while in the possession of UPSI. This implies that even if no trading happens pursuant to such communication, the mere act of communication under UPSI is an offence under the regulations. In addition to an insider communicating the UPSI, procurement of UPSI by any other person is also treated as violation under the regulation and the SEBI keeps a close watch on all such activities. To ensure adherence to the overall compliance programme, completeness in identification of all employees who have access to UPSI is very critical. Further, it is to be ensured that no external threats e.g. cyber-attacks, malware, etc. exist in an organisation, and insider threats through the following modes are minimised:

Eavesdropping

Team member overhearing conversations and privy to UPSI information. Many a time work is done in an open office layout and not in control rooms, war rooms or areas with limited or restricted access.

Extended teams

Outsourced vendors, including printers, IT service providers etc. They could have access to the information but may not be covered through PIT coverage defined by the companies.

Ever connected

Online presence and ability to use various messaging applications which are encrypted and communication cannot be monitored by companies.

Emails

Delegation of emails to junior staff and the possibility of information leakage through this channel.

Espionage

A mole in this team is placed there by the competition or third parties for vested interests. Inadequate background checks of outsourced staff or company staff make this a possibility.

Recent actions of the regulators clearly show that UPSI is being monitored. The regulator is also investigating complaints of individuals spreading UPSI through messaging applications and other mediums.

While regulatory safeguards are in place, companies are expected to:

- Strengthen the key pillars of people, process and technology to avoid leakage of UPSI
- Identify the present system and controls on UPSI, ensure responsibility of who manages such controls and periodicity of such reviews
- If required, conduct an appropriate enquiry or investigation.

Safeguarding UPSI

Preservation of UPSI and ensuring that data doesn't fall in the wrong hands is critical for a company to ensure continued investor confidence, preserving its own good reputation and goodwill in the market. Both these factors go a long way in ensuring smooth sailing for the company in a volatile market scenario, increased regulations and scrutiny.

It is imperative for companies to document the policy and process used to manage UPSI and ensure a comprehensive audit of the same from time to time. Red flags, if identified, from the audits should be documented and steps should be taken to mitigate the risks.

Additionally, companies may look at implementing a few good practices, as indicated below:

Invest in the right technology to:

- Avoid data leakage through IP-based controls, blocking of keywords, recording calls and restricting usage of mobile phones
- Avoid storing sensitive data over the internet or a public online storage space
- Encrypt and password-protect sensitive files
- Ensure physical security and encryption of data stored on computers
- Strengthen the procedures of data and data holding assets in storage and physical transit through the use of offline and online encryption methods.

Invest in the right processes such as:

- Prepare an indicative list of what can be UPSI and circulate it to all employees
- Use only official emails/channels to share information and avoid public emails
- Try to create a separate work space with secured access to teams working on preparing financials during the 'non trading window'.

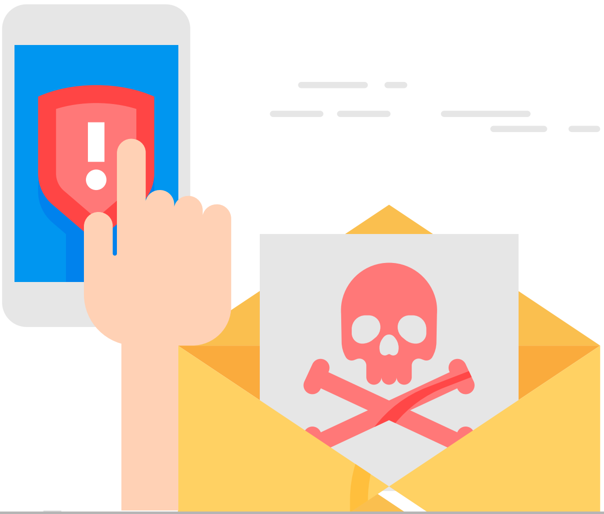
Invest in people control to:

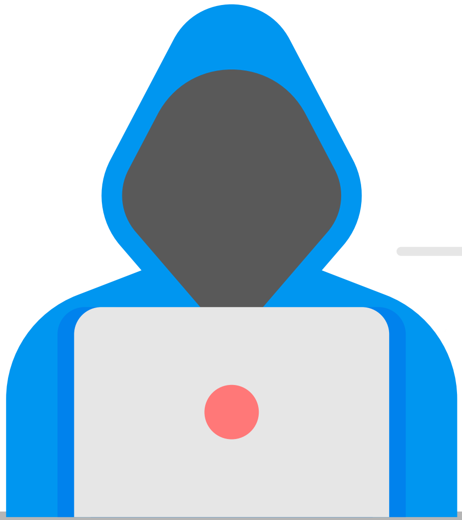
Identify persons involved in major deals/ activities and instruct them not to share any sensitive information beyond that set of people. Ensure that information is percolated down to junior members or external teams only on a 'need to know' basis

- Ensure proper background checks are in place for staff dealing with UPSI data
- Inculcate the culture to report any attempt of breach and conduct refresher training sessions around the sensitivity of the role played
- Monitor any significant price changes just before the declaration of financial earnings for any significant fluctuations proactively.

At the end, investigate as appropriate to ensure there is no exposure. Perhaps an innocuous failed login attempt locking a user account or a social taping to fetch sensitive information could be your next breach!

(With contributions from Suveer Khanna, Partner, Forensic Services, KPMG in India Sudesh Anand Shetty, Partner Forensic Services, KPMG in India)





Opinion

Cyber preparedness can propel your business towards new avenues of revenue growth

Cybersecurity challenges have grown manifold in the Indian business landscape with increasing digitisation and interconnected business operations. The adoption of new technologies is exposing organisations to cyber-attacks, leading to loss of data and resulting in reputational hazard. To ensure protection against cyber threats, cyber security in India has gained importance over the years.

A well-structured and high-quality cyber preparedness programme will not only focus on keeping the data safe and secure but will create trust, boost consumer confidence and have long-term impact on earnings. It will also help to maintain the integrity of data to make sure that right and complete data is available upon which business decisions can be based.

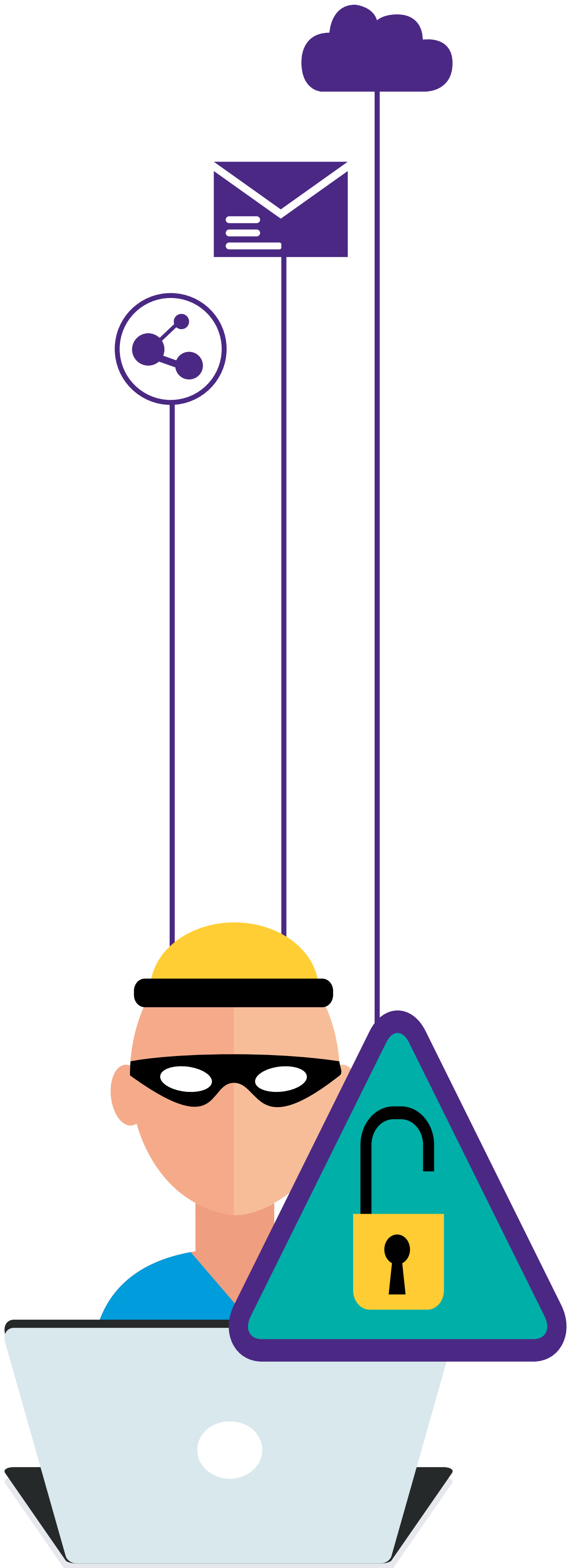
The current Indian business environment is riddled with perils of data theft and the threat is constantly increasing with the proliferation of data. Any information, whether it is customer data, intellectual property (IP) or financial information, is valuable for business and a source of revenue stream. However, in case of a data breach, it can lead to loss of trust, negative publicity, proprietary information, trade secrets and consumer / investor confidence.

What until now was considered an area for reduced spending as it does not directly impact productivity or profit margins is now being viewed as a boardroom priority.

Boardroom discussions today, are increasingly focussed on cyber security. However, detailed discussions on cyber risk, the costs and consequences of IP theft, cyber espionage, data destruction, or business disruption are limited as they are harder to quantify. Cyber breach can have huge repercussions on the business.

Atul Gupta

Partner
IT Advisory
Leader - Cyber Security
KPMG in India



Cybersecurity has emerged as one of the key business risks, and boards are addressing this proactively. Cyber-attacks are a reality in today's world and there is a need for an organisation to have a balance between protection and response measures. Currently, the response preparedness to cyber-attacks needs to be enhanced significantly.

According to KPMG in India's CEO Outlook report 2017, over 89 per cent of Indian CEOs agree that mitigating cyber-risk is now at the top of the boardroom agenda.

The report also suggests that 84 per cent of CEOs plan to increase investment in cybersecurity over the next three years. Interestingly, cybersecurity is no longer seen as a protection cover, but a means to increase revenue. Close to 76 per cent of the CEOs see investment in cybersecurity as an opportunity to find new revenue streams and innovate, rather than view it as an overhead cost.

KPMG in India's Cybercrime survey report 2017 reveals that 18 per cent of organisations are of the opinion that they are fully prepared to withstand and respond to large-scale cyber-attacks, while 69 per cent of organisations are in the process or have formalised cyber response processes and procedures.

It is heartening to note that Indian businesses have made substantial progress in terms of cyber preparedness. About 45 per cent of the CEOs feel they are prepared for a cyber-attack, up from 17 per cent in 2016. Given the level of existing investments in cybersecurity, the level of preparedness is expected to only increase in the near future.

CEOs should understand the real benefits of cybersecurity preparedness

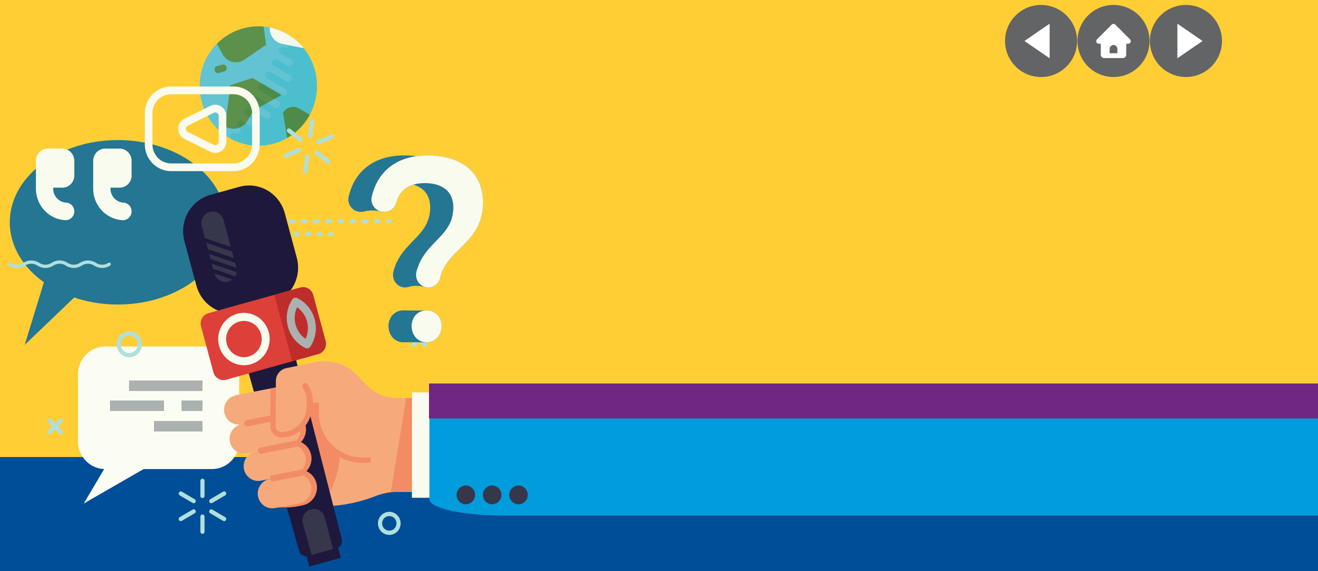
It will require maturity and ability on the part of the CEOs to keep pace in the wake of rising incidents of cyber breaches. A smart cyber strategy which can be understood, accepted and implemented, and which can guard the organisation against cybersecurity threats and potential damage to its reputation, is the need of the hour.

The way forward

It is important to provide a better understanding of specific cyber risks to the CEOs so that they can make more informed decisions aligned with their business strategies. It becomes crucial to understand and prioritise cyber threat intelligence processes, and see how they can be integrated into an organisation's security operations in a way that adds value.

If designed and implemented well, a good cyber strategy can actually help deliver higher revenue and accelerate growth of businesses. Cyber preparedness can actually propel organisations towards new avenues of revenue growth.

KPMG in the News



Trust should not be taken for granted in our profession: KPMG's Bill Thomas | Interview with The Economic Times - On the sidelines of the Economic Times Global Business Summit – 27 February 2018

"We have a great business here and Arun Kumar (India head) has done a tremendous job. For KPMG, the size of the Indian team is only second to the US team." - ***Bill Thomas, Chairman, KPMG International***

Global business community very bullish on India: KPMG | Interview with CNBC TV 18, 27 February 2018

"I think and certainly the clients that I talk to are very bullish on India and where it is at and where it is headed, he said. People want to do business here and historically it has been challenging. The easier it gets, the more interest there will be," he added. - ***Bill Thomas, Chairman, KPMG International***

India must not get complacent, continue with reforms: Bill Thomas, KPMG | Interview with ET Now, 26 February 2018

"Well, the beauty is that India is the fastest growing economy in the world right now. FDI is at an all-time high. There is no doubt that there is momentum in this country. And, momentum creates more momentum. What's important is to deliver on these expectations. It means that you do not get complacent and you continue to push for these 'ease of doing business' kind of reforms." ***- Bill Thomas, Chairman, KPMG International***

View: India must continue to recalibrate to take its seat at the top table for global business | Opinion article in The Economic Times, 21 February 2018

"The Indian economy is moving in the right direction with initiatives taken towards stepping up infrastructure investment, labour market reforms and measures to boost manufacturing growth. However, more reforms will be vital for sustainable growth. While all of this is still an 'unfinished agenda,' a combination of supportive global growth, improving capex, fiscal spending, a buoyant consumer and concerted policy will be crucial in strengthening India's growth outlook." ***- Bill Thomas, Chairman, KPMG International***

Featured publications

Expedition 3.0 — Travel and hospitality gone digital

India's travel sector has expanded in the recent years, driven by the increase in domestic spend, internet penetration and availability of smartphones. Technology today plays a ubiquitous role in shaping the travel industry. This paper attempts to portray an immersive view on the trends, challenges and consequences of digital travel, painting a holistic picture of the unfolding digital travel revolution.

Click here for the report

Learning on point 2018

Developing talent, a mission critical priority for organisations, continues to challenge corporate India. Jointly led by KPMG in India and National HRD Network (NHRDN) , the study, covering 138 leading Indian organisations across sectors delves deep into their learning space, seeking answers to difficult questions. What is ailing the industry? Which factors are working well? This is a first-of-its-kind, India based research, which quantitatively assesses the state of learning and development.

Click here for the report

Transformation of on-road automobiles to electric vehicles in India

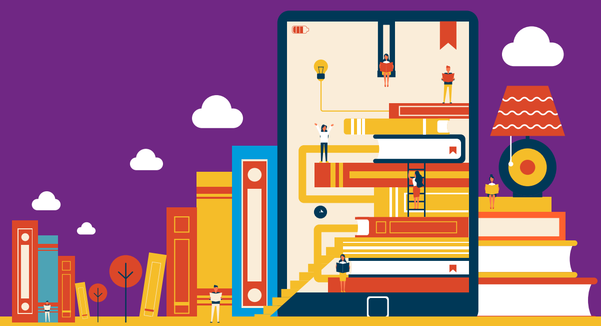
The report attempts to understand the negative impact of internal combustion engines on energy security, economy and environment in India. It looks into regulatory aspects of current mitigation measures being adopted by the government and explores the available options of future mobility in India. It discusses the mobility ecosystem for pure electric vehicles and hybrids/ plug-in hybrids, and how hybrid retrofit kits can serve as transitory technology in achieving full electric mobility in the future. The report also suggests potential policy and regulatory measures for efficient transformation of on-road vehicles into electric vehicles in India.

Click here for the report

India's CSR reporting survey 2017

India's CSR reporting survey 2017 analyses and brings together findings from CSR reporting of the top hundred (N100) listed companies as per market capital as on 31 March 2017. All these companies are required to comply with the requirements of the Corporate Social Responsibility (Policy) Rules (The Act). Their CSR policy, CSR committee, disclosure on CSR in the annual report, CSR spends and others were reviewed based on the availability of information in the public domain as on 30 September 2017. A comparative analysis has also been presented to track the progress as compared to the last two years.

Click here for the report



KPMG in India contact:

Mritunjay Kapur
National Head, Markets and Strategy
Head - Technology, Media and Telecom
T: +91 124 307 4797
E: mritunjay@kpmg.com

KPMG.com/in

KPMG in India 25 YEARS of making a difference

Follow us on:
kpmg.com/in/socialmedia