KPMG

India Insights

The Indian economy newsletter

December 2016

India at a glance

Q2FY2016-17

Macroeconomy[1]

- India continues to recover strongly led by an improvement in terms of trade, effective policy actions and stronger external buffers
- GDP growth in H1FY16-17 was largely consumption driven (especially urban consumption) and a rise in government spending
  - GDP expanded by 7.3 per cent in Q2FY16-17 vis-à-vis 7.6 per cent in Q2FY15-16
  - Investment activity reduced with Gross Fixed Capital Formation (GFCF) contracting 5.6 per cent in Q2FY2016-17
  - Demonetisation could affect growth adversely for the rest of this fiscal year with its impact on consumption

Government finances

- **Fiscal deficit** during the seven months from April to October 2016 was INR4.24 trillion (USD61.91 billion), or 79.3 per cent of the budgeted target for the fiscal year ending in March 2017[3]
- **Trade deficit** widened on a sequential basis to a 10 month high to USD8.34 billion in September led by higher imports of oil, gold and non-gold segments[4]

Foreign Direct Investment (FDI)[5]

- **FDI** equity in India increased by 30 per cent during Apr-Sep 2016 over corresponding period last fiscal

Forex[2]

- **Forex** reserves stood at USD370.76 billion as on 23 September 2016 – continues to be healthy

Disinvestment[6]

- Government has managed to rake in INR210 billion through stake sales buybacks in H1FY17, the highest ever first half disinvestment revenue for the year

Ease of doing business

- Ministry of Corporate Affairs (MCA) has made incorporation easy for companies in India. This was notified as Simplified Proforma for Incorporating Company Electronically (SPICE) in the Companies (Incorporation) Fourth Amendment Rules, 2016.
- The government has set up five committees to review data for GDP estimates, provide mechanisms to ensure data integrity and come up with industry-wise and geography-wise disaggregated data

1. Estimates of Gross Domestic Product for the second quarter (July - September) 2016-17; Central Statistics Office; MOPSI; 30 November 2016
2. Weekly Statistical Supplement; RBI, accessed on 26 August 2016
3. Key Economic Indicators; Office of Chief Economic Advisor; DIPP; accessed on 26 August 2016
4. F2017 Fiscal Deficit Target at a Risk? India Economics - Macro Indicator Chartbook; Morgan Stanley Research; accessed on 23 August 2016
5. Factsheet on Foreign Direct Investment (FDI); Quarterly Factsheet ; DIPP; accessed on September 2016
6. Cabinet gives in principal nod to disinvestment and strategic sale of PSUs; Business Standard; 27 October 2016

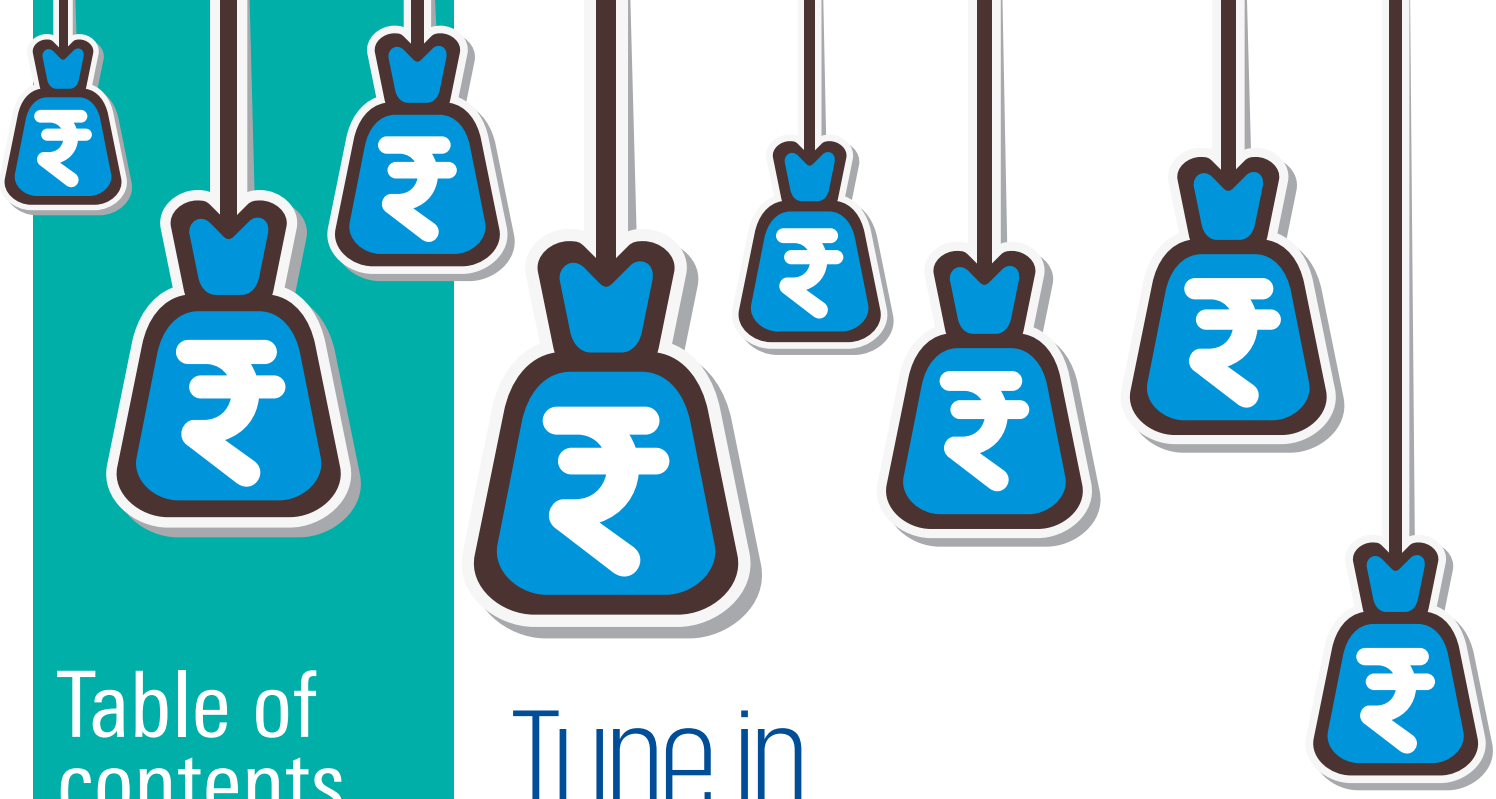


Table of contents

Tune in

Demonetisation - a transformational reform to curb black money

In a special address to the nation on 8 November, Prime Minister Narendra Modi announced that INR500 and INR1000 notes will seize to be accepted as a legal tender after midnight. The demonetised currency is being gradually replaced by a new series of the INR500 note and an all-new INR2000 note, beginning 10 November 2016.[1]

Considered by many as a transformational reform, the measures aim to 'clean up' India's booming economy of untaxed cash transactions that give way to corruption, counterfeit currency and funding of terrorist activities and groups.

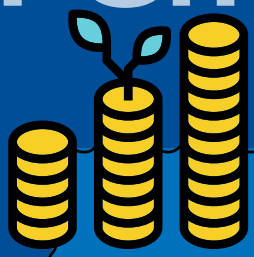
The government earlier this year introduced the Income Declaration Scheme that required citizens to declare their income amassed through various sources. It was an appropriate time, therefore, to make credible the threat of a crackdown on India's parallel economy, which accounts for nearly 20 per cent of the GDP and operates with near impunity.[2]

All measures under the demonetisation drive may be considered akin to a forced disclosure as it lays down well defined limits on deposits, withdrawals and exchange of old currency. Further, the government has provided an alternative opportunity under the Pradhan Mantri Garib Kalyan Yojana to pay taxes with a penalty on their undisclosed income and come clean. This will not only provide additional revenue to the government for undertaking development activities but the legitimate part of the declared income will find its way into the formal economy.

At present, India has one of the highest levels of currencies in circulation at over 12 per cent of Gross Domestic Product (GDP).[3] Of this cash, 86 per cent is in the form of INR500 and INR1000 notes (as of 31 March 2016), both of which have been demonetised.[4] With this sudden currency wipe-out, economic activity is expected to be negatively impacted in the near term. However, the negative effect is likely to be outweighed by significant structural benefits in the long run.

1. Activity at Banks during November 10 to November 18, 2016; Reserve Bank of India; https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=38643; accessed on 21 November 2016
2. India's black economy shrinking, pegged at 20 per cent of GDB: Report; The Indian Express; 5 June 2016
3. The political economy of demonetising high value currency; The Hindu; 15 November 2016
4. CRISIL Research – Insights – Significant Structural Benefits on the cards for India; 9 November 2016

Tune in



Below are the probable consequences on the various economic variables and entities

Inflation

- Slowdown in demand could create excess capacity (due to unutilised capacity), leading to deflationary pressure

Macroeconomic

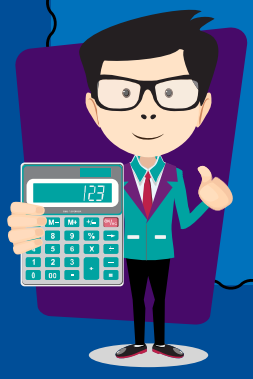
- Improved transparency and tax compliance may encourage higher capital flows (Foreign Direct Investment/ Foreign Institutional Investment)
- Increased financial penetration and enhanced financial savings
- Improved fiscal management due to lower borrowings
- Reduce transaction cost between buyers and sellers

Taxation

- Tax to GDP ratio could witness considerable increase
- Government's tax revenue collections, its ability to spend on infrastructure investments and the resultant impact on growth could be substantial

Banking

- Sudden increase in bank deposits may lead to reduction in interest rates
- NPA and demand for working capital credit may grow
- Borrowings from NBFCs are expected to shore up, especially for accommodating lifestyle expenses and discretionary goods that are usually purchased on credit



Tune in

Parallel economy

- Ease of doing business could improve with systematic reduction in black money circulation
- Illegal funding of anti-social elements are anticipated to see a dip
- Value of counterfeit notes could extinguish
- Demand and price of gold may see a dip as cash reserves dies down

Aggregate demand

- Cash-based sectors may see a sharp moderation
- Discretionary/big ticket items may see a dip in the near term
- **Severely impacted:** Real estate, auto, cement, steel, banks, non-bank financial companies, consumer discretionary and telecom
- The move on black money is likely to result in demand destruction in organised real estate as well as individual/ rural house construction, which may get transmitted to cement demand in due course
- **Moderately impacted:** Consumer staples and e-commerce

Online payment

- Innovation in the nascent electronic payment industry may get a fillip
- Use of digital currency and payment systems driven by UPI, wallets and cards could create enormous transparency and pave way for faster evolution of Fintech companies in India, especially in transactions and online lending space
- Cash on Delivery (CoD) orders are likely to fall for e-commerce companies
- POS terminal usage may increase for the retail segment

Money supply

- Supply of money could decrease permanently to an extent that black money, which is not counterfeit, may not enter the system

It wouldn't be wrong if we said, India is undergoing an economic transition right now; the demonetisation move that initially appeared to have paralysed the economy, is now catalysing the country's 'Digital India' initiative. The digitally startled common man is now keeping aside his wad of cash and signing up for e-payments and mobile wallets.

Needless to say that the top guns of the payment processing companies are overloaded and are racing to accommodate the immense spike in traffic. However, with an increasing velocity and volume of the traffic flowing through, parallel attention needs to be given to infrastructure and security solutions that minimise potential cyber and related threats. Payment companies need to scale up their technology models such that, sudden surge in demand can be managed effectively without compromising confidential data.

Insights

In conversation with our cybersecurity expert

Akhilesh Tuteja

Partner and Head,
Management Consulting and
Global Co-Head for Cybersecurity,
KPMG in India

Q In your view, what are the key challenges that Indian businesses could face over the next five years in the cybersecurity landscape?

Much alike customers, governments and organisations, fraudsters are following the speed, flexibility and convenience that technological integration offers. In a nutshell, the speed of fraud is positively co-related to the pace of technology integration.

A large number of organisational processes in India continue to be largely disintegrated. This limits the level of business exposure available to attackers. However, over the next five years, gaps in cross-channel linkages across Indian businesses are likely to narrow down considerably, exposing all critical channels to attacks of much higher severity, leading to an outrageous collapse of the entire system.

For instance, power distribution companies are prone to much advanced attacks that could lead to collapse of the entire supply chain within no time.

In the current state of affairs, most companies are able to determine the loss when an attack has already taken place and considerable damage has been inflicted upon clients and operations. The challenge that lies ahead for companies is to devise ways that can detect attacks as they are happening, and before the attacker has an opportunity to cause the damage.

If this approach is to be successful, speed is essential. It is not enough to look at the rear-view mirror to understand what happened yesterday. We need a 'front window shield' to analyse, understand and respond to threats as they occur.

Q Which are the key areas where Indian businesses are predominantly investing in cybersecurity solutions and combat measures?

Until recently, large Indian organisations invested a considerable amount of their security resources in threat prevention processes and technologies. These investments only focused on the first few steps of the attack lifecycle — preventing (blocking) the attack from delivering the malware and gaining access to a system.

Further investments have been made in deploying end-point protections such as installing antivirus software, patching software vulnerabilities, and blocking malicious IP addresses and URLs. This approach and the associated processes/technologies were probably adequate for a singular component or automated threats, but do not take into account the multiple steps associated with sophisticated advanced attacks.

Yes, strong security controls are still important, but organisations should now assume that attackers will circumvent defences, penetrate networks, compromise systems, and advance their attacks. Given this, large organisations should supplement attack prevention with a more thorough strategy for threat detection and incident response. This entails getting integrated insights into all activities across networks, hosts (e.g., endpoints and servers), applications, and databases. It also includes monitoring, alerting, analysing for incidents, and then coordinating, containing, remediating, and sharing threat intelligence. Unfortunately, threat detection, investigation, and response in large number of organisations in India remain relatively immature and manually intensive.

Investments should now be more on integrated strategies that can dive into the root cause of the incident, contain and remedy them rather than on different technologies that only see isolated aspects of an attack and lack the bigger picture.[1]

1. An Analytics based approach to Cybersecurity; ESG Solution Showcase, May 2015

Insights

Q When it comes to big data analytics for cybersecurity insights, which sectors could be at the receiving end?

Secure cyberspace has become an indisputable need. With increasing data intensity in organisations, big data analytics is anticipated to be of paramount importance to nearly all sectors of the Indian economy. It can help organisations strengthen their early threat detection strategies and incidence response mechanism. However, this benefit comes at a disproportionately high amount of investments. Sectors/organisations that can allocate large portions of their security resources on acquiring such trained professional and capabilities, are likely to reap benefits.

At present, sectors that could leverage valuable customer insights to pro-actively diagnose and mitigate threats could be end-to-end financial payment companies, including both banking and non-banking companies, payment wallets, healthcare and internet companies.

Q What factors can determine India's rise as a cybersecurity power?

In my view there are two key ingredients that could determine India's rise as a cyber-power:

- **Cutting-edge research**
  Today, individuals, organisations and governments rely and thrive on a web of information that has been made more mobile and flexible by the power of the internet. Computer networks have evolved with those needs, becoming more complex and porous. There are multiple ways in and out of networks, enabling users connect remotely from anywhere in the world and share information quickly with thousands of people at a time. All of this is critical to an efficient business environment. The security that defends those networks, however, has not evolved at the same speed.[2]

  For defence mechanism that could curb complex and evolving threats, Indian companies need to invest in cutting-edge research. India's IT industry needs to build capabilities to think like attackers while devising appropriate defence mechanisms.

- **Vast pool of trained professionals**

  Investments are also required to train and nurture a vast pool of cyber professionals with capabilities to devise new measures and monitor the existing ones.

  India is endowed with a vast pool of trained cyber professionals. In fact Government of India (GOI) and NASSCOM aims to take the cybersecurity industry market share in India from 1 per cent of the IT-BPM industry to 10 per cent by 2025, with a trained base of 1 million certified cybersecurity professionals, as well as build over 100 security product companies in India.[3]

Q Can cybersecurity capabilities be a strategic differentiator for Indian companies?

In my view, companies should not use their cybersecurity capabilities as a strategic differentiator in any manner. This could in turn send out wrong signals to the fraud community and increase their exposure limits considerably. Companies should rather focus on determining their state of readiness for responding to a threat incidence. This can help them strike the right balance between investment and protection strategies. In addition, understanding of a number of key concepts, selection of an appropriate supplier of cybersecurity (incidence response) expertise and an eye over future developments in the evolution and response to cyber threats could be key.

2. Why we must build an immune system to ward off Cyber threats; Live Science; 10 September 2015
3. Nasscom sets-up cyber security task force to build India as the Cyber Security Hub; NASSCOM

Spotlight

Atul Gupta

Partner,
IT-Advisory and Cybersecurity,
KPMG in India

Analysing India's cybersecurity preparedness v/s other global countries

Cybersecurity focuses on having a structured framework that needs to be followed to protect organisations and enterprises against cyber risks. It is targeted on critical information leakage and compromise for malicious reasons.

At present, **cyber has become a Boardroom agenda.** Consequently, management has started taking measures in allocating dedicated budget towards cybersecurity measures and frameworks. There are multiple technology-led approaches which are being deployed to enhance cybersecurity preparedness, such as Security Operation Center (SOC), Identity Access Management (IAM), Next Generation Network Devices (Firewalls), etc.

A cybersecurity framework needs to be developed based on the information assets that shall be under attack (crown jewels), understanding of potential cyber threats, such as viruses and other malicious code, and potential attackers with their motives. The framework shall have a combination of methods, including preventative, detective and response measures to cyber incidents. Cybersecurity strategies include multiple elements, including identity management, risk management and incident management.

As per the Cybercrime report published by Norton Security last year, on an average Indians are losing INR16,558 compared to the global average of INR23,878 to cyber-thieves. Below are the top findings:[1]

Measuring cyber losses

Top Findings	India	Global
Amount consumers lost to cybercrime in the 2014	INR1,882 billion	USD150 billion
Average amount of time consumers lost dealing with the impact of online crime	30 hours	21 hours
The average number of passwords and types of accounts consumers share	2 accounts Email 60 per cent Social media 54 per cent Bank account 36 per cent	2 accounts Email 55 per cent Social media 43 per cent Bank account 27 per cent
Respondents who are confident they know what to do if they become a victim of online crime	40 per cent	30 per cent
Millennial who say they aren't "interesting enough" to be a target of online crime, despite having experienced it	Millennial who say they aren't "interesting enough" to be a target of online crime, despite having experienced it	Millennial – "I'm not Interested". 38 per cent Experienced online crime. 56 per cent

1. Norton Cybersecurity Insights Report Global Comparisons; Symantec Corporation; 2015

Spotlight

The exposure from cyber risk is expected to increase exponentially with adoption of emerging technologies, including mobile devices, remote working, Internet of Things (IoT) and increasing digital transformation across the country and enterprises. As per Ken research, it has been expected that by 2020 there would be an increase in number of connected devices to 2.7 billion in 2020 from around 200 million presently.[2]

India Inc. has taken multiple steps to address cybersecurity risk by devising regulations/ guidelines, including the Information Technology Act, National Cyber Security Policy, National Privacy Law and Companies Act. Simultaneously, industry regulators have also brought in various requirements, including RBI's guidelines for security, IRDA's insurance security, TRAI's telecom network security, etc.

India cyber preparedness - challenges and road ahead

Globally, in a study performed by ITU, India ranks fifth on the Global Cybersecurity Index (GCI), which represents the preparedness of the country to deal with cybersecurity threats. These measures are distributed among the following five areas - legal, technical, organisational, capacity building and international cooperation.[3]

Country	Index	Global Rank
United States of America	0.824	1
Canada	0.794	2
Australia	0.765	3
Malaysia	0.765	3
Oman	0.765	3
New Zealand	0.735	4
Norway	0.735	4
Brazil	0.706	5
Estonia	0.706	5
Germany	0.706	5
India	0.706	5
Japan	0.706	5
Republic of Korea	0.706	5
United Kingdom	0.706	5

2. Digitisation initiatives by government, increasing online transaction and compliance led deployment of security solution in SMEbusinesses to boost cyber security market in India; Ken Research; May 6, 2016
3. Global Cybersecurity Index & Cyber wellness profiles; ITU; 28 May 2015

Spotlight

The below table presents India's preparedness against other countries in legal, technical, organisational, capacity building and cooperation towards cybersecurity.[3]

Asia-Pacific	Legal	Technical	Organizational	Capacity Building	Cooperation	Index	Regional Ranking
Australia	0.7500	0.6667	0.8750	0.8750	0.6250	0.7647	1
Malaysia	0.7500	0.8333	1.0000	0.6250	0.6250	0.7647	1
NewZealand	1.0000	0.8333	0.8750	0.6250	0.5000	0.7353	2
India	1.0000	0.6667	0.7500	0.7500	0.3750	0.7059	3
Japan	1.0000	0.6667	0.7500	0.7500	0.6250	0.7059	3
Republic of Korea	1.0000	0.6667	0.8750	0.8750	0.5000	0.7059	3
Singapore	0.7500	0.6667	0.7500	0.7500	0.5000	0.6765	4
Honk Kong	0.7500	0.6667	0.5000	0.7500	0.5000	0.6176	5
Indonesia	1.0000	0.3333	0.2500	0.5000	0.5000	0.4706	5

Despite the fact that India is positioned better in comparison to other countries, there are multiple challenges which the country faces due to increased exposure of corporates and citizens of country to cyber-attacks. The following trends are observed in the country:

Internet usage:

One of the major factors which leads to uncontrolled expansion in the usage of internet worldwide is mobility. The advent of mobile devices has brought an unimaginable number of users online. This has exposed them to increased risks associated with cyber space, where many of them may be first time users of internet and may not be skilled enough to understand the risks. This introduces a platform for hackers to steal personal and corporate information which are sensitive in nature.

Advanced technologies:

The emergence of advanced technologies (cloud, analytics, etc.) is another key factor which is responsible for increased risks. Organisations are rapidly moving towards cloud based solutions due to increased computing and storage needs. The information gets exposed when the safeguards for cyber risks are not appropriately designed during adoption of these technologies.

Lack of awareness

Another top concern is ensuring data leakage prevention. The stakeholders are unaware regarding the criticality of data housed in the organisation; the data remains unclassified and unmanaged. Lack of awareness regarding dataflow leads to unauthorised access and loss of valuable information.

Lack of employees with cybersecurity skills and awareness has emerged as another major reason why organisations are unable to defend themselves against cybersecurity attacks. This impacts the organisation's ability to identify, contain and mitigate cybersecurity incidents, leading to severe losses.

Social engineering:

Attacks (phishing, identity impersonation on social media, etc.) has emerged as one of the key risks. As per Symantec's report on financial threats, 2016, globally, India ranks third in terms of being vulnerable to Trojan-infections.

IInitiatives being taken by Indian government to enhance cybersecurity posture across country:[4]

- India has an active Computer Emergency Response Team (CERT-IN) that effectively collaborates with key players in the field of security and educates consumers on cybersecurity issues.

3. Global Cybersecurity Index & Cyber wellness profiles; ITU; 28 May 2015
4. Current Scenario; Cyber Security Strategy; Ministry of Electronics and Information Technology; accessed on 5 December 2016

- Government has set-up an Inter Departmental Information Security Task Force (ISTF) with National Security
- India's National Cyber Security Policy is in the implementation phase. The purpose of this framework document is to help ensure a secure and resilient cyberspace for citizens, businesses and the government.
- National Cyber Security Task Force (CSTF) has been created by NASSCOM under the mandate of Prime Minister Office to address various domains of cyber risks.[5]
- India is undertaking a number of research and development projects in the areas of:
- (a) Encryption techniques, (b) Cybersecurity incident response, (c) Network and systems security assurance, (d) Cybersecurity resilience plans, (e) Cyber forensics and (f) Capacity development in the area of cybersecurity

5. NASSCOM sets-up cyber security task force to built India as the cyber security hub; NASSCOM

Future of cybersecurity

With increased growth in cybersecurity incidents, governments and organisations around the world are becoming more and more aware of security measures to be taken in order to defend themselves against cyber-attacks. India as a country is strongly moving forward with its vision of 'Digital India' and also simultaneously taking up the measures to tackle the cyber threat. There are many cybersecurity initiatives which are envisaged at country level (statutory requirements) and from industry regulators.

Enterprises need to look at cyber risk as a business risk rather than only technology risk and address it in holistic manner. There are global frameworks which can be aligned to the requirements of the organisation, and the key will be to bring in all elements, including people, process and technology.

The attacks shall continue and the preparedness/ response for these attacks shall also continue to change, since this is a dynamic environment. This peculiarity has brought in increased need of cyber professionals and considering the current state this domain is providing huge opportunities to task force that intends to build their profile in cybersecurity.

Market trends

Mritunjay Kapur

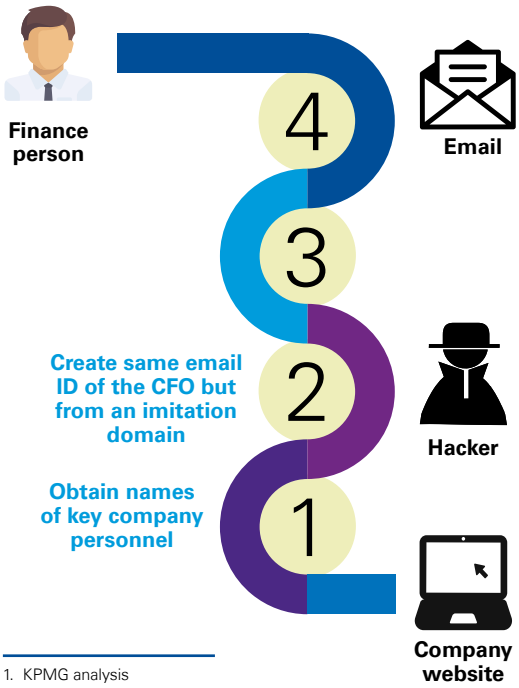
Partner and Head,
Risk Consulting,
KPMG in India

Emerging cyber-threats and response mechanisms

Over the last two decades, the world has seen rapid strides in technology and communications. In a digital world, cybercrime is evolving rapidly, making it one of the biggest threats to businesses, individuals and governments. KPMG India's Cybercrime Survey Report 2015 reveals that 94 per cent respondents view cybercrime as a major threat to business.

In India, cybercrime syndicates have mushroomed at an alarming rate along with tools of online deception to attack enterprises. And yet, surprisingly, a significant number of Indian businesses continue to remain unprepared or are inadequately prepared to deal with these risks.

Modus operndi :Spear phishing[1]



1. KPMG analysis

Recent trends in cybercrime

The cyber fraudster is deftly adapting to the evolutions in technology to commit cybercrimes that are harder to trace, wider in reach and devastating in impact. Some techniques used by criminals to target corporates in India are as under:

Ransomware attacks:

Malicious employees or external hackers steal or lock out sensitive corporate data demanding ransom (usually in the form of virtual currency such as bitcoins) for secure destruction or unlocking of the same. Failing to pay the ransom may lead to the employee/hacker releasing the data in the public domain. This can lead to the employer facing penalties on account of confidentiality breaches or fines from regulators. Ransom ware such as Reveton, Zepto, Cryptowall were known to restrict access to computer, systems and demand that the user pay a ransom to the malware operator to remove restrictions imposed by these ransom ware.

Spear phishing

The typical modus operandi of the fraudster is to first identify potential target companies and gather information about the key personnel (usually from websites, social media websites). They then register a domain name that looks similar to the target's domain address. An e-mail account is then hosted and used to send forged e-mails posing as CFO or CEO. These e-mails are sent to the finance directors or managers instructing them transfer funds to an international bank account and charge the amount to admin expenses. Fraudsters typically target hundreds of companies with customised e-mails. Several corporates are known to fall prey to these types of attacks.

Fund diversion attacks

The typical modus operandi of this attack involves implanting Trojans in computers of key personnel in accounts receivables department or the companies e-mail server with a view to obtain the credentials of their e-mail accounts. Using the Trojan, the cyber fraudster monitors the e-mail flow between the victim and the customers over a period of months. At an opportune time, the hacker strikes by impersonating the victim and directly communicating with the customer. The customer is asked to remit funds into an unknown account, which is instantly emptied using international laundering syndicates.

Conclusion

Cybersecurity has emerged as one of the most important concerns for businesses. The sophistication and rapid growth of cybercrimes cannot be ignored. Corporates should bear in mind that an effective cybersecurity strategy, is not a onetime activity but a continuously evolving cycle of activities that need to be carried out at periodic intervals. These include:

- Development of a Cyber Fraud Policy Framework (including incident management, enhancement and assessment)
- Cyber fraud controls design and review
- Cyber forensic incident response investigation.

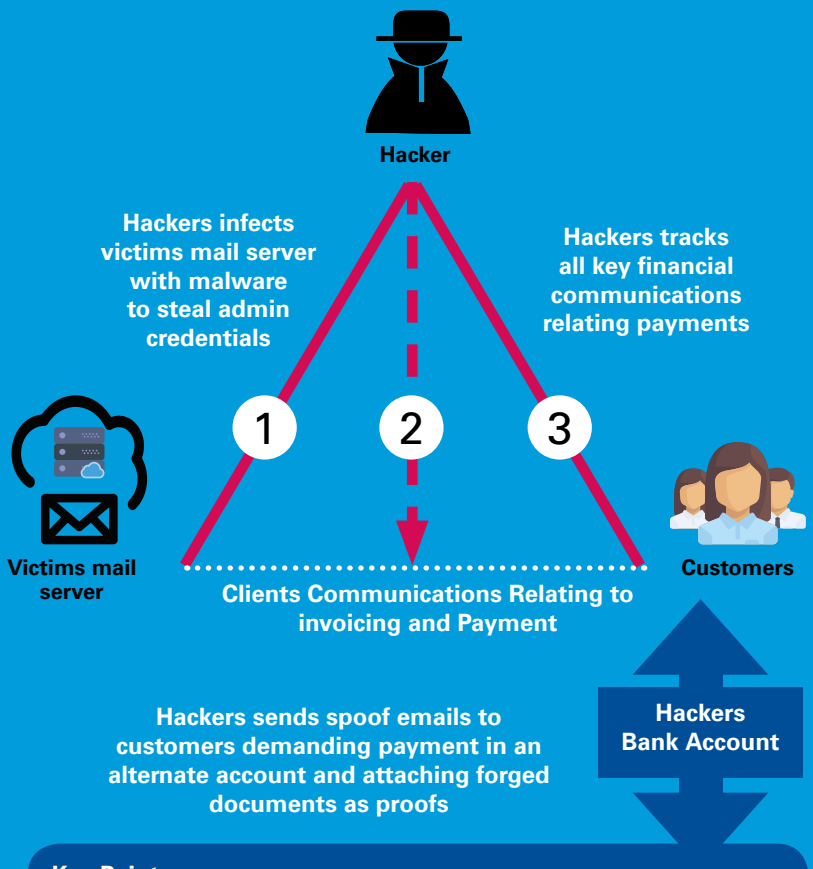
Further, detective/monitoring technologies should be adequately utilised for timely detection of cyber-attacks and employing adequate countermeasures and corrective controls.

While the above is a sound framework for cyber risk management, the key ingredients for success of such a framework are:

- Boards/senior management of organisations should take cognisance of the internal threats in their organisations
- Adequate support from the management
- Development of adequate cyber response mechanisms

Last, the sustainability of such cyber risk management programmes requires tireless efforts to be put into creating and maintaining continuous awareness among end users. As the saying goes, you are only as strong as your weakest link.

Modus operndi :Fund diversion attacks[2]



Key Pointers

- Spoofed domains from which emails are sent are hosted outside India and owned by persons not residing in the hosting country
- Hackers accounts are emptied and closed as soon as funds are received
- Accounts are usually outside India and at multiple companies

2. KPMG analysis

In the NEWS

The imperatives of a high-performing Board; Mint; 3 November 2016

Based on surveys and interactions with business leaders, KPMG's Business Leadership Centre highlights four imperatives for Boards to perform under pressure. Corporate Boards are constantly under pressure to improve their performance by expanding both the areas they oversee and the intensity with which they oversee these areas. Prescriptive regulations, empowered shareholders who challenge corporate decisions and a competitive environment that has blurred the distinction between an ally and a competitor have added to the pressure.

Sustaining talent practices crucial to organizational growth, success; Mint; 17 October 2016

India continues to excel in the visionary and strategic leadership and financial management, according to our Management Capability Index. KPMG in India in collaboration with AIMA (All India Management Association) presented the fourth edition of the Management Capability Index (MCI) India 2016 survey—a leading research on the progressive capability of organisations. The MCI, a thorough measure, helps professionals evaluate their business performance and identify growth indicators.

Malware alert! Extortion now very much in digital world; The Financial Express; 6 November 2016

"Ransomware comes on the system in a disguised format (known as a Trojan) such as an attachment in an e-mail, a file downloaded from the internet and so on. It appears to be harmless. However, the malware has hidden logic (called payload), which works in the background and encrypts the information on the system," says Atul Gupta, Partner, IT advisory and Cybersecurity, KPMG in India."

Kerala among most vocal states on GST council: The Hindu Business, 30 October 2016

Kerala has been among the most vocal states in the GST council. "By taking the lead in spreading awareness on GST, the state has reiterated its commitment to implement the same,"

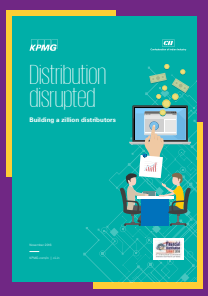
Sachin Menon
Sachin Menon, Partner and Head, Indirect Tax, KPMG in India.

Featured publications

India's food industry: Growth receipe

The food services industry in India has witnessed unprecedented growth over the past few years. However, it still faces a lot of regulatory challenges as the current laws mandate new businesses to obtain a number of permits to become operational. This KPMG India–FICCI joint report looks into insights on the current challenges related to policy and regulatory aspects, and edifies the readers about the ease of doing business scenario in the industry. The report also delves into key focal development areas to address the skill gap challenge and other bottlenecks. A thorough study is followed by key recommendations as the next steps to address various issues faced by the Indian food services industry to make it globally competitive.

Click here for the report



Distribution-Disrupted: Building a zillion distributors

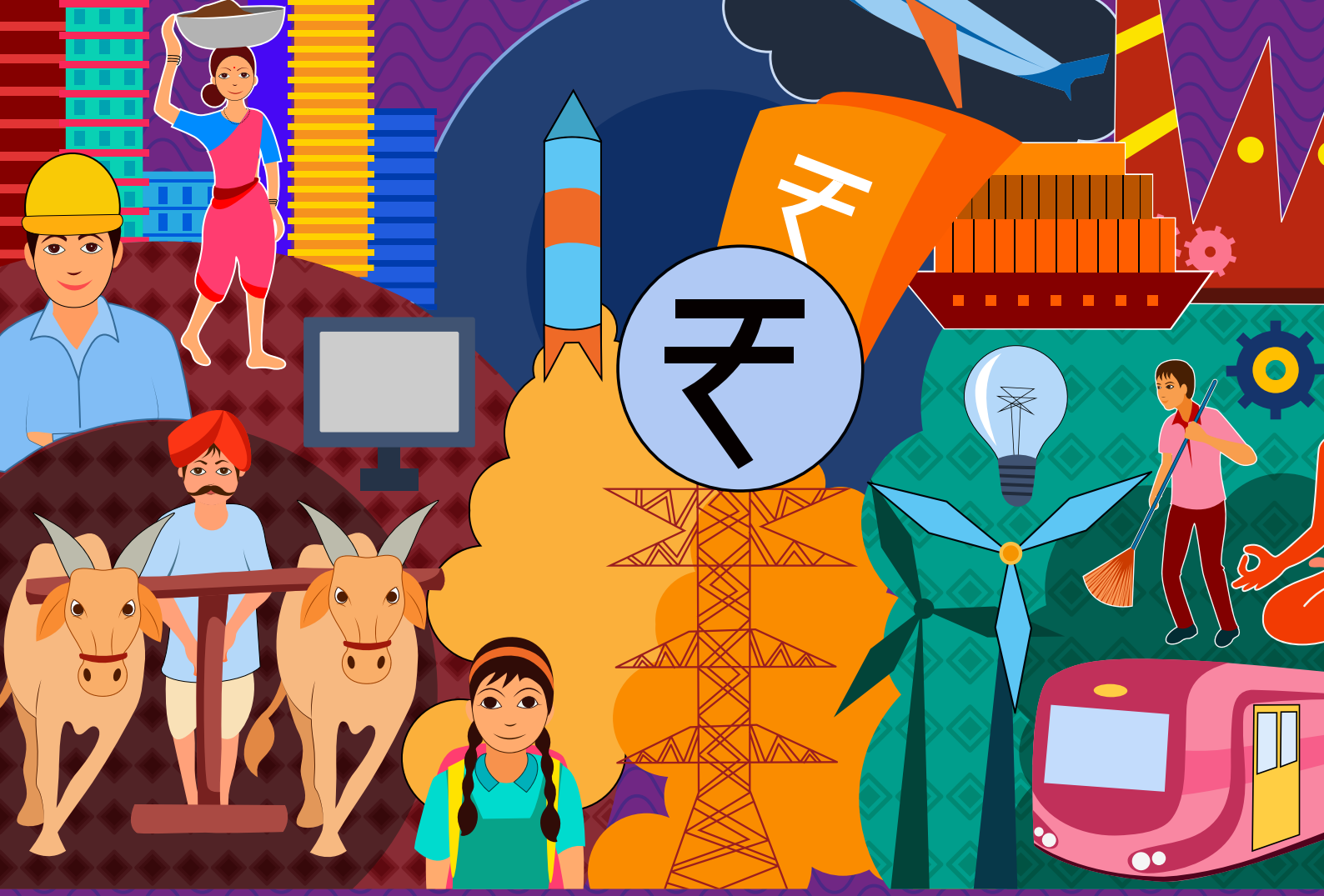
This report by CII and KPMG in India unravels the current market potential for financial products in India with a spotlight on the Indian financial distribution ecosystem along with its pertinent challenges and methodologies; amidst evolving technology and regulation.

Click here for the report

ENRich 2016: Point of Views

The energy landscape is likely to see unprecedented transition and transformation driven by energy security, climate change, technology, and consumer behaviour. Organisations will need to be prepared for these changes. Our seventh annual energy conclave, 'ENRich 2016', deliberated these subjects, implications that this will have on stakeholders' and how businesses are working towards overcoming some of these challenges facing the sector

Click here for the report



KPMG in India contact:

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

KPMG.com/in

Follow us on:
kpmg.com/in/socialmedia

Download the KPMG India application:

Download on the App Store