

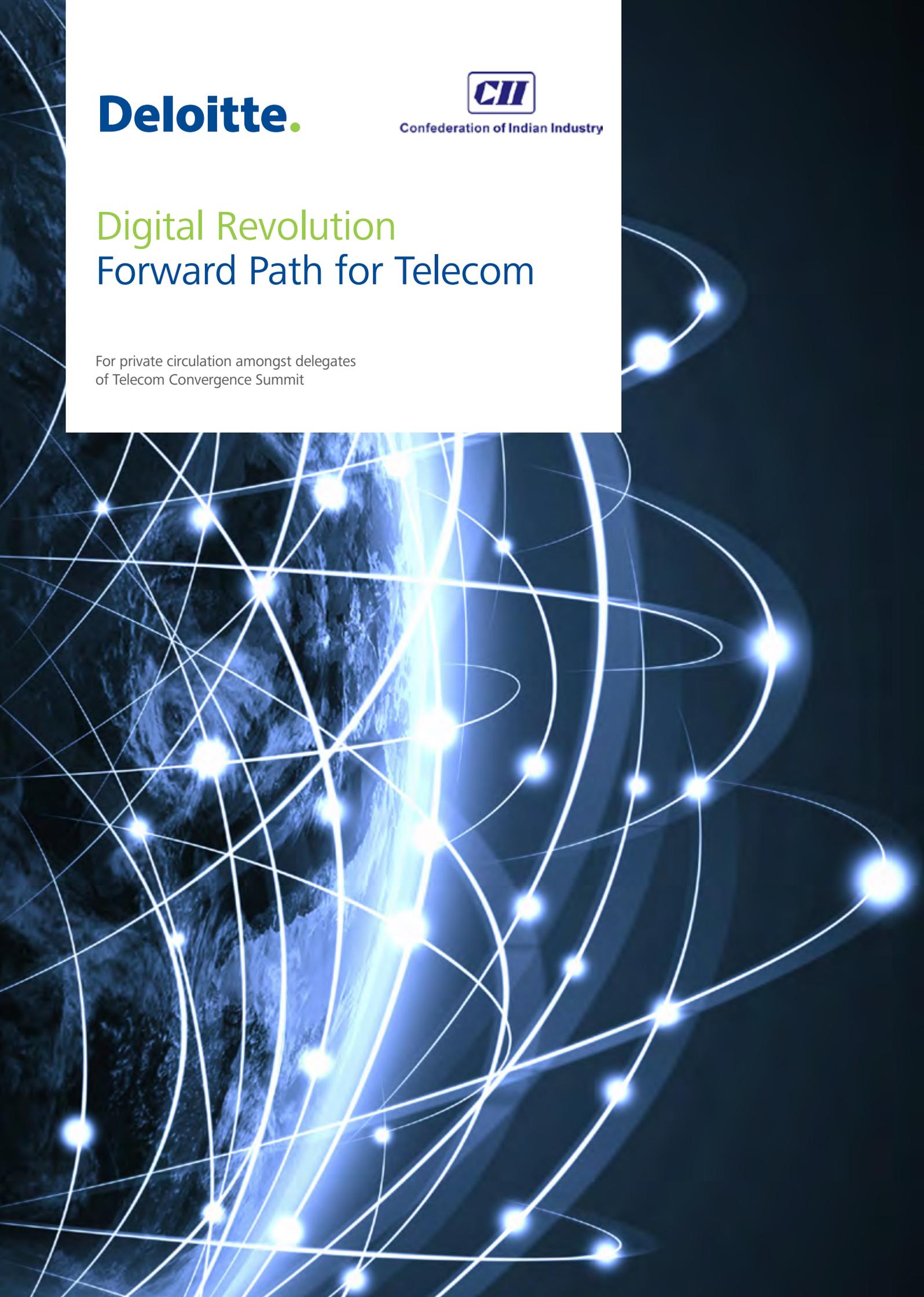
**Deloitte.**



Confederation of Indian Industry

# Digital Revolution Forward Path for Telecom

For private circulation amongst delegates  
of Telecom Convergence Summit



# Contents

Foreword	3
Message from CII	5
Internet of Everything: Is there a limit?	6
Net Neutrality: What is in it for me?	11
Digital Commerce: What the future holds?	15
Cyber Security: Is there a middle way?	19
Evolving Technology: Can India afford to be left behind?	27
About Confederation of Indian Industry	33
Acknowledgements	34
References	35

# Foreword

Digital revolution is the backbone of economic, technological, and social prosperity after the industrial revolution. It is driven by high-speed Internet connectivity and innovative products and services. The transistor which was invented in 1947 paved the way for digital revolution. Advanced computers helped the government, military and other organizations to solve critical problems efficiently. The creation of World Wide Web helped revolutionize the communication systems and made internet an essential part of every business. The medium of communication has changed rapidly and mobile communication has become an inevitable part of life. The internet users rose as mobile devices enabled easy and faster connectivity. Instant messengers and chatrooms replaced the voice communication while e-commerce is bringing a paradigm shift in the way people shop. We are now getting into the era of Internet of Things and Augmented Reality.

New technologies based on mobile connectivity, social media, cloud computing and big data are leading the way, driving efficiency and productivity. Creative business models of organizations along with innovative products and services are driving consumer demand, creating job opportunities and empowering employees. It is also enabling the society to use resources more efficiently while making the national economy more competitive. Traditional businesses and digitally enabled organizations are no longer constrained by geographical boundaries due to digitization. To sustain and grow further, companies have started embracing digital transformation as they find it difficult to compete with the new age entrepreneurs. Low barrier to entry, minimal cost of innovation, faster customer reach, and product adoption have given strong momentum to the digital revolution.

India has a pool of young talent with almost 50% of the population below the age of 30 years. It has the largest non-internet users in the world with almost 1 billion population remaining offline. Connecting a country of 1.25 billion people with high speed internet can help in bringing together the academia, research institutions, industry, government, startups, and others to drive innovation and solve many perennial problems faced by the country. Indian government would be spending around \$18 billion for digital revolution in the country. The government and private organizations by focusing their efforts on extending the digital technologies will enable equitable and inclusive growth of the rural and remote communities as well.

Although there is no end to connecting people, things and sensors, thoughtful choice and purpose of connectivity should be the broader focus of the organizations to create value, keeping in mind the social norms of fairness, objectivity and justice. This enhanced connectivity also exposes companies, individuals, and the society to greater cyber threats and attacks. It calls for a new cultural approach of shared responsibility that is integrated into almost every aspect of public and private life as a commitment towards cyber-safety. One should always keep in mind that technology is for making our life easier, faster, and secure, but if this has reverse effect on the way we work, live or learn, it is time to change the controls of digital masters.



**Hemant Joshi**



# Message from CII

The telecom industry around the world is redefining communication services more frequently than ever. The bandwidth promised by newer technologies is setting new benchmarks rapidly. Every new technology is superior to the former one by 100 or even 1000 times.

Digital commerce finds place in everyday news for many reasons like new ventures, creative business models, funding, valuations, market offerings and profitability. Some of the segments such as electronics, insurance, and travel booking have a substantial online platform presence while other segments like pharmaceutical products, automotive, machinery are still inclined towards traditional business models.

The convergence between telecom and information technology means that there needs to be innovation, competition, and investment in the telecom networks, as well as in the services, content, applications and operating systems. The success of each of these players in the digital ecosystem depends on the success of the other.

The e-commerce market is witnessing huge domestic and foreign funding from various investors. This segment is expanding large capital on marketing, supply chains, logistics, and talent. The valuations of the companies are growing with every new round of funding. No matter how high the valuation of an e-commerce company is, its profitability is still unestablished.

Hereby wishing all the success to CII Telecom Convergence Summit which will deliberate on some of the topical issues of the Sector and help charting a roadmap defining the growth path in the times to come.



**Mr Umang Das**

Chairman

CII TELECOM Convergence Summit 2015

# Internet of Everything: Is there a limit?

It is no news to us that we live in a connected world. Following statistics from Cisco about connectivity trends in India only bolsters this thought further.<sup>1</sup>

- 47.3 million net new devices and connections were added to the mobile network in 2014.
- 51% of mobile connections will be 'smart' connections by 2019, up from 8% in 2014.
- The number of wearable devices will reach 5.9 million in number by 2019, up from 1.4 million in 2014, a CAGR of 34%.
- The number of mobile-connected M2M modules will grow 6.9-fold between 2014 and 2019, reaching 47 million in number.

---

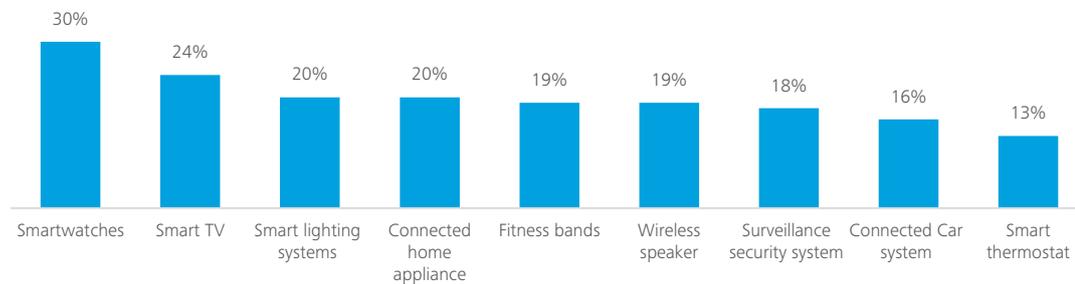
“The Internet of Things (IoT) is expected to be the next big thing in the mobile ecosystem and a key driver for further growth in cellular. Numerous services are planned for IoT over cellular networks, including utility meters, vending machines and automotive applications. There are already some IoT services use cases we see around, such as wearables. It is expected that the use of wearables consisting of multiple types of devices and sensors will become mainstream. Smart services will become pervasive in urban areas, and usage will also grow in suburban and rural areas. In the coming years, mobile video surveillance may evolve to be available on aircrafts, drones, cars, and safety and security personnel for monitoring houses/buildings, targeted areas, special events, etc. However, low cost connected devices, enhanced coverage coupled with support of device volumes are some key requirements for cellular to enable these services to have mass adoption.”

– Amit Marwah, CTO, Nokia Networks India



The IoT is estimated to create business value of up to \$511 billion over the next decade in India. This includes \$394.4 billion in the private sector and \$116.2 billion in the public sector.<sup>2</sup> IoT technology is creating opportunities in unexpected places and ways, including Internet-connected wearables, insurance policies, retail supply chains, connected cars, etc. A similar sentiment is reflected in Deloitte Global Mobile Consumer Survey where significant number of people from urban areas has shown willingness to purchase smart devices in the next 12 to 18 months.

**Figure 1: Willingness to purchase smart devices in next 12 months**



Source: Deloitte Global Mobile Consumer Survey 2015 - India results

### Government initiatives

The government is taking proactive steps to build the IoT capabilities in India and facilitate the development of ecosystem in various possible ways. Department of Electronics and Information Technology (DeiTY) has come out with a draft IoT Policy document which focuses on creating an IoT industry in India of \$15 billion by 2020. As part of this policy, the government wishes to undertake capacity development (Human & Technology) for IoT specific skill-sets for domestic and international markets. The government has launched The Centre of Excellence (CoE) for IoT in Bangalore to enable rapid adoption of IoT technology and foster new growth strategy as well empower India to have a leap frog advantage in the domain. The CoE will be run on a Public Private Partnership (PPP) model with seed fund from the government and will be managed by NASSCOM.<sup>3</sup> It will undertake research & development for all the assisting technologies and help develop IoT products specific to Indian needs in all possible domains.

The Indian Government’s plan of developing 100 smart cities in the country, for which ₹70.60 billion has been allocated in the current budget could lead to a massive and quick expansion of IoT in the country.

### What it means for Telecom Operators

Cisco predicts that \$14.4 trillion of value (net profits) will be “at stake” for private-sector businesses globally over the next decade (2013-2022), driven by IoT.<sup>4</sup> Given the scale of opportunity, few organizations would refrain from developing connectivity and intelligence in the products.

IoT offers telecom operators two-sided benefits:

1. IoT offers new avenues to significantly boost their revenues. Certain products or services that were earlier considered to be expensive and unviable are now possible to develop and deploy with the help of IoT.
2. IoT helps in improving productivity and save costs, such as capex, maintenance, labor, and energy. For example, Verizon is saving more than 55 million kWh annually across 24 data centers by deploying hundreds of sensors and control points throughout the data center, connected wirelessly. The result is a reduction of 66 million pounds of greenhouse gases per year.<sup>5</sup>

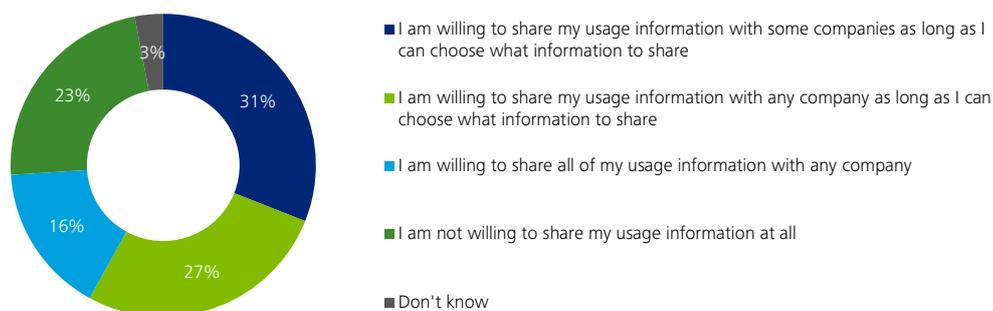


The success of IoT will need both technical and business model innovation. Telecom infrastructure needs to be upgraded or expanded to carry traffic of billions of connected devices. To derive full potential of the IoT technology, telecom coverage across the country even in remote and rural areas will play a fundamental role. On the other hand, the devices that will communicate through these robust networks also need to be installed with high quality sensors, chips, batteries and software. Having seen the problem of high power consumption in smartphones and tablets, it is critical to develop low power IoT devices. So to capture a disproportionate share of IoT value and to have distinct advantage in serving the market, telecom operators will likely have to deliver lower-cost and lower-power communication services.

There is an endless list of use cases for IoT that an operator can work on. However, telecom operators cannot imagine having all the capabilities across required across industries such as medical devices, automobiles, supply chain solutions, etc. in-house. It will be very important for all players in the value chain to cooperate and work together to develop use cases that will solve real problems and generate measurable results. These could act as the specific business priorities for them. Hence, telecom networks will need to be built with features and security parameters that will define the future of IoT and complementary applications.

It will be easier for operators to upsell their IoT products as they already provide broadband and mobile connectivity to homes and offices. As more and more consumer products get connected to the internet, telecom operators will need to build trust and loyalty with the customers who would be now seeking multiple services. This trust will need to be built over time as most of the customers seem to be willing to share usage information generated by the devices they own.

**Figure 2: Willingness to share the usage information generated by your device**



Source: Deloitte Global Mobile Consumer Survey 2015 - India results

Value is created and captured by not only the products and services, but also by the information that these products and services provide. It is this newly gained information that creates business value and provides meaningful insights for future actions. High tech and telecommunications firms realized only 65.4% of the \$118.3 billion IoT value at stake available to them in 2013.<sup>6</sup>

Distributed networks, advanced technology, and new business models not only change technology, but also how individuals approach and accomplish their work. This makes change management a key to completing the story for any IoT application. The major change that the IoT brings is that now the information content of a product is as valuable as its performance. The way in which the resulting information creates value can be understood using a common analytical framework: the Information Value Loop (see inset).<sup>7</sup> The flow of information around the value loop creates value for customers which companies can then capture. Analyzing this flow of information can help telecom operators locate specific strategic and technical challenges facing them in an IoT-enabled world. They should design IoT deployments to create a flow of information around the value loop most relevant to a given business priority.



### The Information Value Loop

The suite of technologies that enables the Internet of Things promises to turn almost any object into a source of information about that object. This creates both a new way to differentiate products and services and a new source of value that can be managed in its own right.

Creating value in the form of products and services gave rise to the notion of a “value chain”—the series and sequence of activities by which an organization transforms inputs into outputs. Similarly, realizing the IoT’s full potential motivates a framework that captures the series and sequence of activities by which organizations create value from information: the Information Value Loop.

Note first that the value loop is a loop: An action—the state of behavior of things in the real world – gives rise to information, which then gets manipulated in order to inform future action. For information to complete the loop and create value, it passes through the stages of the loop, each stage enabled by specific *technologies*. An act is monitored by a sensor, which creates information. That information passes through a network so that it can be *communicated*, and *standards*—technical, legal, regulatory, or social—allow that information to aggregate across time and space. *Augmented intelligence* is a generic term meant to capture all manner of analytical support, which collectively are used to analyze information. The loop is completed via *augmented behavior* technologies that either enable automated autonomous action or shape human decisions in a manner that leads to improved action.

The amount of value created by information passing through the loop is a function of the value drivers identified in the middle. Falling into three generic categories—magnitude, risk, and time—the specific drivers listed are not exhaustive but only illustrative. Different applications will benefit from an emphasis on different drivers.



Graphic: Deloitte University Press

Identifying where the bottlenecks lie, how each party is motivated to respond, and seeking to shape both incentives and the value loop itself puts companies more in control of their destinies.



### Countries leading in the IoT race

Several countries like the US, South Korea, China among others have taken the lead in their preparedness for taking advantage of IoT. Japan had developed the u-Japan Policy early in 2004 to accelerate the realization of network access ubiquity for smart devices.<sup>8</sup> The telecom industry has high hopes for the IoT as it is expected to boom in sectors such as telemetering, transportation management, e-payment, surveillance, digital signage, and data backup, thereby bringing huge business opportunities by creating new areas of growth in the saturated Japanese mobile market.

China has benefited from proactive government support in the development of the IoT with funding allocated as part of the country's 12th Five-Year Development Plans and additional funding made available for research and development. China has also led in the development of standards, establishing an IoT standards association and promoting Chinese-developed standards internationally. The Chinese government has also selected 202 cities, to pilot smart city projects to collect, store, and analyze information related to transportation, electricity, public safety and environmental factors.<sup>9</sup>

The Alliance for Internet of Things Innovation (AIOTI) was initiated to assist the European Commission in the preparation of future IoT research, innovation and standardization policies. It is also going to play an essential role in the designing of IoT large scale pilots, which will be funded by the Horizon 2020 Research and Innovation Programme. The members of AIOTI will jointly work on the creation of a dynamic European IoT ecosystem.<sup>10</sup>

In Singapore, the government authority is working with industry and public sector partners to develop a Smart Nation Platform (SNP), which comprises a connectivity layer and a sensing and IoT layer.<sup>11</sup>

### Going ahead

India has strong capabilities in the supply side (information technology, manufacturing, telecommunications and digital services) and the demand side (health care, transport, retail and utilities).

Although the government has taken steps to promote IoT, policy makers may need to allocate more resources to improve telecom infrastructure to enable IoT use. Also along with the government, telecom service providers will need to work with the technology companies and research institutions to establish standards for interoperability and security between sensors and connected devices that are proliferating across, homes, offices and public places. Industry, academia, government and research institutions should together develop prototypes for some critical use cases where it would be easier to deploy at large scale and see fruitful results for the benefit of all players.

An estimated 11 billion sensors are currently deployed around the world in power grids, vehicles, offices, and homes. But most of these aren't connected to a network, let alone to the Internet. The challenge is not only to connect these sensors but to decide which of the 1.5 trillion objects in the world should be connected and for what purpose. The question really is - How connected do we really want to be? What all do we want connected? What is the purpose of getting connected?

The goal should not be connecting everything; it should be the network of appropriate things, deliberately chosen and purposely deployed.<sup>12</sup> Understanding of the things that will genuinely improve our lives, save money, conserve natural resources, or drive better efficiencies will be critical to the IoT realizing its full potential. Consequently, the bottleneck currently in India is at the Create stage of the loop due to the lack of an appropriate application of sensor technology. Whoever controls the bottleneck is typically best positioned to capture a disproportionate share of the value created.

Thoughtful choice and purpose should be the broader focus of the organizations. Real impact, business or social, will come from combining data and relevant sensors, things, and people. Within the ecosystems, organizations need to think carefully about questions of value capture: how to share value with customers and other partners in the ecosystem in ways that respect both economic needs and social norms of objectivity and justice.

When the bottleneck they control is relaxed, where will it be next, and how will that affect them? Without this strategic foresight, one might end up simply creating value that others capture.

# Net Neutrality: What is in it for me?



Net Neutrality is a term that was coined in 2003 by Columbia University Media Law Professor Tim Wu. It is the principle that: "Internet service providers - and government - should treat all data on the Internet equally, not discriminating or charging differentially by user, content, site, platform, application, service, type of attached equipment, or mode of communication". Practically this means that: Internet service providers should not depart from the traditional best-effort packet forwarding approach and differentiate the speeds with which packets are delivered and should not block access to websites by establishing walled gardens or similar kinds of limits on the content, applications and services that can be accessed by Internet users.

Some of the well-known incidents of violation of net neutrality are: Brazil and Germany's leading telecom operators blocked Skype, a VoIP service, because of its competition with their own national and international roaming services. ISPs in France and UK throttled YouTube at peak times.

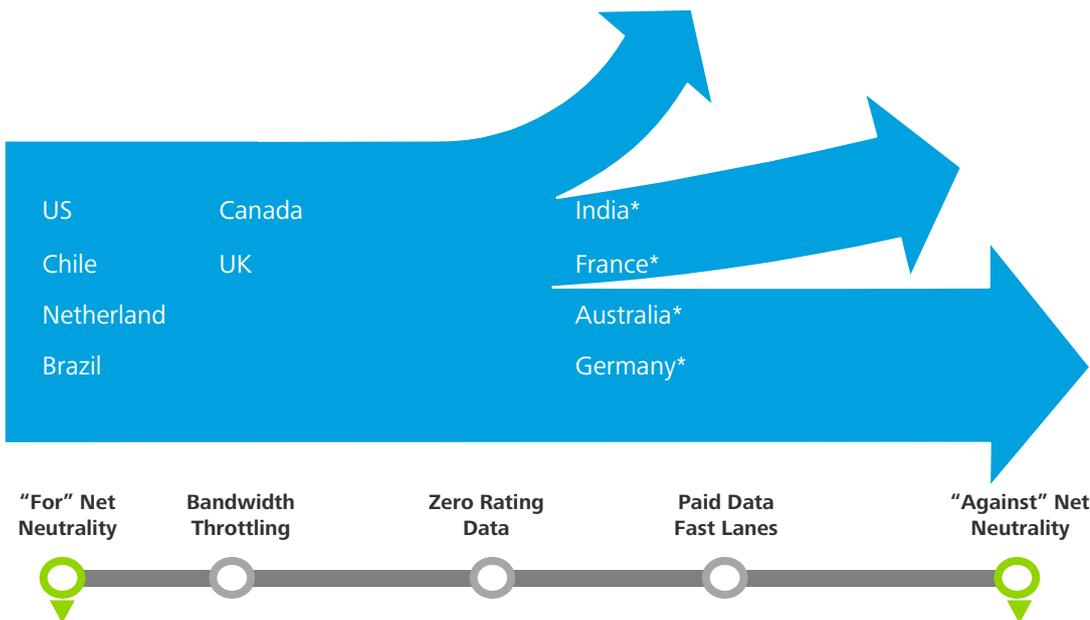
In addition to real incidents of Internet blocking and censorship by network operators, governmental interference with the Internet content has become increasingly common as well e.g. The PRISM surveillance program in the US.

Such blocking of access to Internet resources by network operators is not only motivated by economic gains most of the times, but also could be by government mandates, attempts by third parties to mount lawsuits against Internet service providers, or an attempt to save networks from cyber-attacks.<sup>13</sup> Similar to network operators not owing liability around who talks and what they talk about using the operators networks, operators also do now owe liability for what content is streamed on their networks.

## Net neutrality debate spectrum<sup>14</sup>

The net neutrality debate spectrum (ranging from 'for' to 'against') has points of dispute which show where a country or company positions on the broader subject.

Figure 3: Net Neutrality Debate Spectrum



Source: Deloitte Analysis

Note: \* Countries considering specialized services in their proposals on net neutrality



**“Pure Net Neutrality”**, a scenario where data can move unrestricted around the world between networks, where ISPs do not discriminate in any way between different types of data, regardless of the strain certain types of data may place on a network.

**“Bandwidth Throttling”** is the intentional slowing of internet service by an ISP. It is a reactive measure employed in communication networks in an attempt to regulate network traffic and minimize bandwidth congestion.

**“Zero-rating Data”** is where consumers can download certain content and it will not count towards their data limit or is provided free. The ISP or the content provider essentially picks up the ‘data tab’ for the consumer. Leading Australian telecom operator Telstra provides un-metered data for certain types of content (e.g. entertainment, sport, education, health). In the US, T-Mobile’s “Music Freedom” program offers unlimited music downloads for the most popular music services available. “Facebook Zero” and “Google Free Zone” are special ‘zero-rating data’ programs that allow customers to access stripped down content online. These programs are a way to provide services more broadly in developing countries to the poor.

**“Paid Data Fast Lanes”** is a system that would allow ISPs to introduce options where content producers could pay more to have their content delivered to customers faster and more reliably than those that do not pay more. Households could also pay more to have content delivered faster and more reliably than neighbors who don’t.

Proponents of net neutrality are 100% committed to not allowing the introduction of data ‘fast lanes’, while ISPs want the freedom to offer premium services to those that are willing to pay for them.

### Positioning of countries on the net neutrality debate spectrum

#### “FOR” Group

In February 2015, the US regulator Federal Communications Commission (FCC) established “Open Internet Rules” focused on:

1. no blocking of access to legal content
2. no throttling (slowing) of traffic
3. no paid prioritization of traffic
4. reclassifies “broadband Internet access service” as a telecommunications service

The long-term existence of the FCC’s “Open Internet Order” depends on the outcome of legal proceedings from broadband providers and US telecom industry trade associations, who are suing the FCC over the above mentioned new rules. It is a notable fact that the US has strong presence of the technology companies not only in the Silicon Valley, but also in other parts of the country.

Similarly, Brazil, Netherlands and Chile have strong net neutrality laws and have banned zero rating programs for violating the basic principles of net neutrality.

#### Not “FOR” Group

The continuously expanding digital ecosystem can be derived from the following facts from Cisco’s VNI report<sup>15</sup> of 2014:

- The number of mobile-connected devices exceeded the world’s population in 2014. Globally, smart devices represented 26% of the total mobile devices and connections in 2014; they accounted for 88% of the mobile data traffic. This implies the increasing traffic is generating significant pressure on the capacity of current networks. This will further get amplified with exponential growth of Internet of Things (IoT).
- Mobile video traffic exceeded 55% of total mobile data traffic by the end of 2014. This indicates that video is mainly responsible for generating huge traffic compared to voice, file sharing, web browsing, and others.



- According to a mobile data usage study conducted by Cisco, the top 20% of mobile users generated 85% of mobile data traffic, and the top 1% generated 18%. This clearly indicates that Internet user profiles are not homogenous any more.

There is a wide variety of services and applications that can be delivered over the Internet and the traffic generated by video applications such as Skype, YouTube, is far more than the other applications, thus congesting the networks. This has led to the premise that these Information Technology companies should be equally responsible for building the capacity of network infrastructure.

According to analysts, a bandwidth market is not a zero sum game in which any extra bandwidth resources consumed by one user leaves less for others. Similarly, priority delivery by courier delivery services does not slow down their standard delivery; priority delivery should not alter the default delivery speeds on an ISP's network. Considering the analogy of toll highways, even private toll roads do not slow down the speeds of public highways.

Market-driven differential pricing based on capacity usage and quality of service have been the norms in several industries. For example, airlines charge differently for the space usage for 1st class, business, and economy class and provide priority check-in and specialized services according to the class. The hospitality industry charges differently for the size and quality of the room. The amount of the highway toll varies by vehicle type, weight, or number of axles, with freight trucks often charged higher rates than cars. On this basis, the network operators have a rational to charge different applications according to the data traffic generated and the type of connectivity parameters (high availability, reliability, secure, etc.).

**The European Union Council's draft proposal on net neutrality does not prohibit specialized services or fast lanes for priority services. It favors freedom of choice for users, and the need for a commercially differentiated supply.**

Because Internet connectivity does not conform to national borders, net neutrality is really a globally applicable principle that can guide Internet governance. The above examples indicate that the decisions of the government are driven by the commercial interests of the region's businesses and nation's economy.

#### Indian context

The telecom sector has witnessed great success in the last few years and attained the position of 2nd largest market with 900+ million mobile subscribers. The telecom industry continues to grow and is highly competitive with 13 operators fighting for the share of the customer's wallet. It has shown significant progress attracting the second highest FDI among all sectors and stimulating domestic investments.



However, the network infrastructure has not progressed considerably as compared to the growth of data traffic (75% annual mobile internet traffic growth in 2014<sup>16</sup>). This might be due to several factors that the Indian telecom operators face putting them in a unique spot:

- high churn rate
- lowest average revenue per user (ARPU) in the world
- high debt burden (approximately ₹3 trillion)
- declining voice revenues (about ₹0.35 per minute)
- low spectrum per operator (quarter of global average)
- high subscribers per MHz spectrum (about 3.8 million)

The annual growth in Internet users (about 12% growth in 2014) is far less than the growth in internet traffic (about 75%). This indicates that the growth is driven by the content and service providers, leading to the increasing importance of these technology, content, application, and services providers. The app-based communication or the rise of the over-the-top (OTT) players is shrinking the revenues of telecom operators and reducing them to dumb pipes. The instant messenger and VoIP apps are providing calling and messenger services allowing users to call or message directly via internet, thus eroding the revenue streams (voice and SMS) of telecom operators.

### Concluding remarks

The convergence between telecom and information technology increasingly means that there needs to be innovation, competition, and investment in the telecom networks, as well as in the services, content, applications and operating systems. The success of each of these players in the digital ecosystem depends on the success of the other. The connectivity provided by telecom networks in the form of Internet is meaningless without the content and services, and without services and applications, Internet is of no use. Hence, both need to coexist harmoniously and support the sustainability of each other.

It is essential that both can develop sustainably, with equivalent regulations and principles. Meeting certain basic principles in favor of competition and against arbitrary discrimination would create the conditions for fostering the development of the digital ecosystem.

Thus, the regulator needs to consider the following before a policy decision is taken on net neutrality:

- Commercial interests of the telecom and technology companies in India
- The best interests of the citizens of the country
- Maximize total investment across the entire digital ecosystem

The government should ensure that the Internet remains a platform for innovation, economic growth, and free expression and mitigate any issues with flexible and soft regulation, keeping in mind the interests of the nation, its businesses and its people.

# Digital Commerce: What the future holds?



E-commerce and e-tail are no more buzzwords for Indian customers. Since its inception around 1991 and the first major digital commerce website from Indian railways (IRCTC) back in 2002 the sector has crossed many milestones in India<sup>17</sup>. The increased penetration of smartphone users and internet subscribers and attractive payment options with deep discounts has helped the e-commerce players to gain more customers. However, online retail still only accounts for about 2-3% of India's \$600 billion retail market.

Digital commerce finds place in everyday news for many reasons like new ventures, creative business models, funding, valuations, market offerings and profitability. Some of the segments such as electronics, insurance, and travel booking have a substantial online platform presence while other segments like pharmaceutical products, automotive, machinery are still inclined towards traditional business models. India is a large emerging market in terms of population, and organized retail is still underpenetrated. Although urban India has high potential, the population residing in non-urban India consisting of 66% of the country's population, is mostly untapped.

The e-commerce market is witnessing huge domestic and foreign funding from various investors. This segment is expending large capital on marketing, supply chains, logistics, and talent. The valuations of the companies are growing with every new round of funding. No matter how high the valuation of an e-commerce company is, its profitability is still unestablished. Immediate profitability is a major challenge for Indian e-commerce players given the Non-Urban penetration of internet, the intensity of competition, and consumer behavior.

## High potential market

The Internet & Mobile Association of India (IAMAI) estimated the Indian e-commerce market at \$13.5 billion in 2014<sup>18</sup>. Online travel in 2015 is estimated to be \$10.4 billion and e-tail Gross Merchandise Volume (GMV) in India in 2015 is estimated to be \$10 billion. As per Forrester, the total number of online shoppers in India will grow to 100 million by 2016<sup>19</sup>. It is a keenly watched market given the high potential it shows. The skyrocketing valuation of some home grown players in a short span of time has become a topic of interest for angel investors, venture capitalists, Foreign Institutional Investors, Incubators, as well as industry watchdogs.

As per the "Global Retail E-Commerce Index 2015" which ranks top 30 e-commerce markets in the world, India remains unranked while other emerging economies of Brazil, China, and Russia find their ranks among developed nations.<sup>20</sup>

India with 66 million digital commerce users has great potential for growth given the population base of 1.25 billion. The digital commerce reach, which was mostly limited to urban population, is expected to grow through the massive digitization effort in India and plan of building broadband highways. There are several other factors that have the potential to exponentially grow the digital commerce market.

- **Demographics:** Demographics play a major role in digital commerce. Spending patterns, purchasing power and the mindset of consumer vary from country to country. The middle class population in India is the highest user of digital commerce.
- **Non-urban penetration:** ~66% population resides in non-urban parts of India and including these into the e-Commerce market (which mostly consists of Metros, tier-1 and tier-2 cities) will make a huge difference. Financial inclusion programs and the increasing internet penetration are enabling the non-urban Indian digitally. According to analysts, non-urban India FMCG market will surpass \$100 billion mark by 2025.<sup>21</sup> In terms of e-commerce market, non-urban India is mostly untapped because of lack of awareness, logistics, supply chain, and low purchasing power.



- **Rise of m-commerce:** There are about 975 million wireless subscribers in India. The wireless teledensity in urban areas is in excess of 143 while there is still huge potential in non-urban areas with teledensity of 48.<sup>22</sup> A significantly large percentage of this subscriber base in India will be using mobile devices to access internet, estimated at 283 million users as of March 2015 and growing rapidly. This rapid spread of mobile internet, especially on smartphones could unlock a significant market beyond the Tier 1 cities for the online retail segment. Undoubtedly, mobile retailing is expected to continue to grow aggressively. In the next three years, global e-commerce sales made via mobile devices are expected to top \$638 billion.<sup>23</sup> It is estimated that 41% of e-commerce sales in India are driven by mobile.<sup>24</sup>
- **Convenient payment options:** The Cash-on-Delivery (CoD) model, which accounts for 60% of the all e-commerce payments, is the favorite payment instrument for the Indian consumers. The emerging online payment systems, which include payment gateways to pay via credit card, debit card and internet banking along with digital wallets like PayTM, MobiKwik, Google Wallet, not only help in instant money transactions but are also secured. The paperless transaction in India has increased significantly in the last few years. According to RBI data, paperless transactions, including retail electronic transactions such as electronic clearing system (ECS) debits and credits, electronic fund transfer, card transactions, mobile transactions, and prepaid instruments, were to the tune of ₹92 trillion in FY15 while the paper-based transactions were around ₹85 trillion during the same period.<sup>25</sup>
- **Logistics:** India is a vast geography, and logistics will play a key role in the growth of digital commerce. Amazon, Flipkart, Snapdeal and others are keen to leverage the huge network of Indian Post to reach the interiors of India for product delivery and CoD collection. Other courier services are also gearing up for providing end-to-end logistics solutions as they find the partnership with e-commerce players profitable.

#### Key factors in the growth of e-commerce in India

- Significant awareness and acceptability created by e-commerce companies on the back of huge marketing spends and customer acquisition strategies like discounts, offers, free deliveries, high levels of customer satisfaction, etc. Internet shopping is a very common practice for discretionary shoppers, especially in urban areas.
- Pan India demand aggregation using online portals and supply using a combination of centralized inventory and efficient operations, which could lead to significant price benefits to consumers and sellers in the long run. Also, launch of private label brands by companies like Zivame, FirstCry, Yepme has been capital efficient as these companies do not need to provide for inventory in every location that they serve.
- Increasing preference for urban shoppers to shop online to save time and compare products / prices before buying. Online shopping is an easy gateway for tier 2 and tier 3 consumers to have access to niche products like high-end products and international brands.

In 2020, for an estimate of \$100 billion in e-commerce sales, the e-commerce penetration for India could be ~10% of the overall retail market of \$1 trillion.<sup>26</sup> This compares with ~18-20% online penetration in South Korea, 8-10% in the US, and 5-7% in China in 2015.



Table 1: Largest bets in the sector

Company	Sector	Funding (\$) Sept' 2015	Investors
Flipkart	Horizontal e-commerce	3.2 billion	Tiger, Accel, DST, Naspers
Snapdeal	Horizontal e-commerce	1.6 billion	Softbank, BVP, Kalaari, Foxconn
PayTM	Payments + Horizontal e-commerce	635 million +	Alibaba, ANT, SAIF, Intel
Ola Cabs	Cab service	677 million	Softbank, Tiger, Sequoia, Matrix
Quikr	Classifieds	410 million	NVP, Warburg Pincus, Tiger
Housing	Real estate	140 million	Softbank, Helion, Qualcomm, NVP
Pepperfry	Furniture marketplace	128 million	Goldman Sachs, Bertelsmann, NVP
OYO Rooms	Budget hotels	132 million	Sequoia, Lightspeed, Softbank
Practo	Healthcare listing	125 million	Sequoia, Matrix, Sofina, Google
ShopClues	Horizontal e-commerce	116 million	Helion, Nexus, Tiger
FreeCharge	Recharge	117 million	Sequoia, Sofina, Tybourne
Zomato	Restaurant review and ordering	224 million	Sequoia, InfoEdge, Vy Capital
BankBazaar	Financial products	80 million	Sequoia, Amazon, Walden

Source: Venture Intelligence



### What the future holds

1. The valuation for larger companies (as a multiple of GMV) could shrink and eventually move to EBITDA (or profit) based multiples – this will be a turning point for the industry and the operating efficiencies will then dictate valuations. Certain players may stall then, where funding could dry up for smaller companies or where operating efficiencies are not visible. Investors today appear to be largely focused on business model and growth (GMV, customer acquisition, number of app downloads, potential for scalability) and believe that companies will turn profitable with scale – however, this is uncharted territory as of now.
2. Valuation of marketplaces (Amazon, Flipkart, Snapdeal, Alibaba) are governed by GMV as they earn a percentage margin on the GMV. For companies with a large share of own brands (private label) sales, the valuation may need to be adjusted by factoring-in higher Gross and Net Margins.
3. With multiple companies selling the same products (especially electronics and fashion apparel), the customer is likely to stay with the top 5 horizontal portals for his / her generic requirements with category leaders in furniture, baby-care, travel, healthcare, beauty emerging as important players, and possible acquisition targets for the larger players in same industry (horizontal players).
4. Unlike physical retail, me-too players in e-commerce may not be able to sustain due to more efficient pricing and product discovery offered by the large players. Also, product discovery and price discovery portals are likely to emerge as significant players going forward.
5. Payment banks can play a big role in increasing usage of plastic / e-Money which will in turn help digital commerce grow.
6. Virtual wallet providers like Paytm and MobiKwik providing easy and secure payment options will go a long way in increasing the footprint of e-commerce.
7. The perspective on Apps: There are two business models being rolled out by e-commerce websites
  - a) PC + Mobile App: We believe that the reason for going app-only is to compel mobile-users to download the app – this strategy is likely to work for dominant players only.
  - b) Mobile App only: Excluding the option to purchase via PCs could be a severe challenge while making non-standard, significant, or one-off purchases (furniture, household appliances, etc.)
8. Two significant challenges need to be addressed on the delivery front
  - a) Alternate to Cash-on-Delivery (CoD)
  - b) Improving the time per delivery

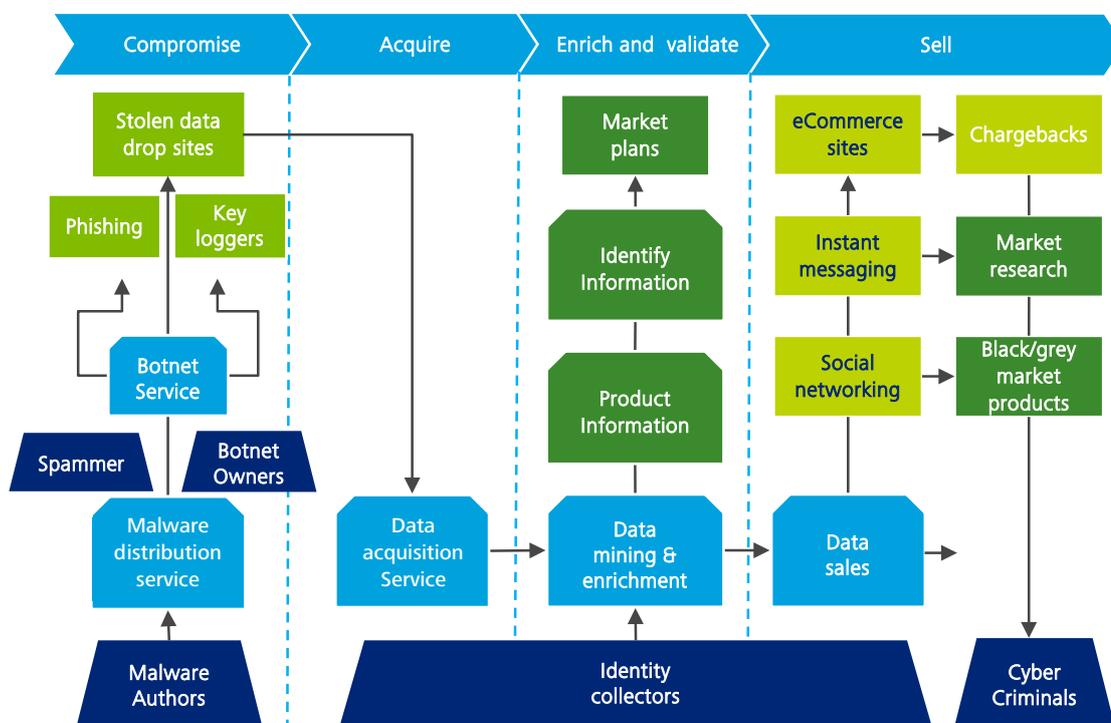
Technology-led solutions (mobile payments, geo-fencing driven alerts, etc.) and scale will be required to sustain free home deliveries. Also, self-pickup could be a relevant play in the near future.

# Cyber Security: Is there a middle way?



Cybersecurity continues to be one of the most pressing challenges facing Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) today. Security threats to government and private organizations have been widely reported: however the nature of the game has changed. Organizations face millions of cyber-attacks every day, whether they know it or not. These attacks are growing in sophistication, magnitude, and number. With the pervasiveness of smart devices, social media, and mobility, organizations are becoming more vulnerable to privacy breaches, fraud, and espionage. Cyber criminals are finding lucrative new markets for selling confidential information.

Figure 4: The underground economy<sup>27</sup>



As organizations (both public and private) progress towards a future of internet-hosted applications using new technologies, like big data, mobile solutions, and cloud computing, and continue to grow their electronic repositories of valuable citizen data, addressing the issue of protecting personally identifiable information (PII) and state systems is of utmost importance.

Today, it's not a question of "if," but rather "when" your network will be breached. This means government agencies and their industry partners must plan and prepare for how to respond to many different scenarios. Today, organizations are considering how to manage their risk in fundamentally different ways. By integrating their information, operations, and risk management activities, organizations can create a more comprehensive, intelligent Cyber-enabled ecosystem to better detect, prevent, respond to, and recover from a wide range of threats.



Organizations in today's modern society need to be more proactive—even pre-emptive—in their ability to detect and confront threats, no matter what their mission. Whether they are delivering services to customers or helping to protect military service members on the front lines of defense, this means developing a cyber-analytics capability to identify emerging threat patterns to anticipate intrusions and developing a cyber-forensic capability to track where attacks originate. These basic building blocks of a cyber-intelligence framework not only help an agency continuously monitor its risks, but also create a more dynamic situational awareness that drives better decision-making across a wider range of mission and business activities.

The main question for ICT organizations today is how to achieve information security. Organizations are taking a close look at their ever-increasing security threats, and then developing/ re-defining their strategies and implementation plans to manage and mitigate the risks more effectively.

#### **Trends leading to increased focus on cyber security<sup>28</sup>**

Cyber security is fast becoming a key concern for telecom industry amid the rapidly changing technology landscape, innovative service delivery models, demanding consumer behavior and more importantly regulatory requirements from various regulatory agencies. The following section provides some insights into the trends and regulations leading to increased focus on cyber security by telecom service providers.

#### **Mobile and Bring Your Own Device (BYOD)**

Today's mobile devices enable employees to work anytime, anywhere, and are powerful enough to handle most business activities and data, including email, documents, contacts, and agenda. They are also used extensively for social media and access to cloud stored data. This intermingling of access to business data and use of personal software applications in one device makes mobile devices a prime target for hackers and provides new entry points for attack. Also, mobile devices are easily lost or stolen. The risks are even greater when employees use their own devices that are not managed by organization's IT department under the policies specific to mobile devices and BYOD.

#### **Cloud computing & rogue IT**

A lot of ICT organizations are already using cloud computing for their critical and/ or non-critical applications. It is important to note that ease of use often trumps security if not integrated/ managed well. In particular, it is often difficult to know where cloud data is physically stored and what national and local regulations apply to it. Cloud also enables increasing occurrence of rogue IT by enabling individuals or groups within the business to easily gain access to software applications that are managed and controlled outside of the organization. In many cases, the internal people responsible for managing information security may not even learn about these rogue applications until their use is too extensive to control. What's more, cloud may increase an organization's vulnerability to third-party security risks. The potential problems multiply when people use mobile devices to access cloud applications and to upload data to the cloud. These combined risks will only increase in the future as mobile and cloud technologies proliferate. Privacy is another people-related challenge exacerbated by mobile and cloud.

---

Stealth techniques enable cyber criminals to act without fear of timely detection, let alone capture and successful prosecution. It is among some of the most insidious—and profitable—of crimes, and can be conducted from a well-equipped workstation, perhaps within your own organization.

---

People are part of the problem when it comes to information security, so they need to be part of the solution. Training and awareness will also help ICT organizations manage the risks from new technologies.



Risk from new technologies is inevitable and constant. The best an organization can do is to create a resilient enterprise by preparing its people for the challenges that are likely to arise. That means raising employee awareness of potential security issues and risks, and training IT and security professionals how to handle the latest threats.

#### **Telecom equipment and networks**

Telecom networks are an integral part of a country's critical infrastructure and act as a backbone in enabling and linking the other critical components such as Energy, Banking, Power, Railways, Aviation, Citizens, etc. This characteristic of the telecom networks make them hot targets for the attackers. Government agencies have been cognizant of this, and over the last few years the telecom regulator has included multiple security conditions as part of the license amendments.

The telecom equipment that is procured and deployed may have malware and/ or bugs having potential to cause information leakage or compromise. The sophisticated attackers of the modern age target these equipment to inflict significant economic damage and public unrest. The extent of such breaches could have substantial impact on the national security. Traditionally, the core telecom equipment hardly underwent rigorous security testing prior to their deployment. However, the current environment demands that these equipment and associated infrastructure be thoroughly tested to eliminate any possible security threat to the organization and/ or to the nation.

#### **Third parties and suppliers**

In today's hyper-connected world of digital supply chains, outsourcing, and cloud computing, ICT organizations are more reliant than ever on third parties. No wonder organizations consider third-party risks and vulnerabilities to be their biggest security threat. After all, a chain is only as strong as its weakest link. As businesses become more reliant on third parties—and as third parties develop their own downstream service networks and increasingly rely on cloud—organizations are finding their data being shared and exposed in ways they don't understand or control. In this hyper-connected environment, a breach anywhere in the digital supply chain can undermine the information security of every organization involved. Despite these rising challenges, many organizations still mainly rely on contracts and similar methods as their primary weapons for managing third-party/ supplier risks.

#### **Mobile apps and payments**

The e-commerce industry is the latest revolution in India. In order to reduce costs and grow business, the e-commerce players are launching new mobile-friendly applications and gradually phasing out the websites, encouraging their customers to make mobile payments. Though this is a win-all business proposition to all the stakeholders, the added dimension of monetary transactions could raise the cyber risk exposure.

---

Organizations need to work with their third parties to understand and improve their combined security capabilities. Contracts alone are not enough.



### **Social media**

Social media has become an integral part of our daily routine. Faster mobile data availability and on-the-move accessibility to social media applications have enabled users to share their information. However, excessive and needless use of social media has resulted in revealing personal and sensitive information to the external world posing privacy-related issues.

---

The question is not if you will be attacked; the question is when — and how you will deal with it. Effective management of information security risks requires a robust combination of prevention, early detection, and rapid response that involves third-party business partners as well as the public sector.

### **Internet of Things (IoT)**

IoT is a great opportunity that can boost the telecommunication sector further as people will be constantly connected to thousands of devices and large amount of data will be generated. While IoT offers unprecedented degree of interconnectivity, it creates countless end-points resulting in huge security threat to the telecom industry. The latest trend on machine-to-machine (M2M) communication where telecom provides the carrier for exchange/ transfer of data between inter-connected machines provides opportunities for the attackers to gain control and/ or modify the operations of the machines, which could lead to substantial losses or damages. A few such incidents have already been reported in advanced automobiles.

### **Cyber security drivers for ICT in India**

The government and related agencies have been impressing to integrate the security at each layer of the business within the ICT. The current government has emphasized to provide Cyber security the utmost importance to combat any possibility of Cyberwar. The government over the last few years has taken necessary steps to enhance the cyber security measure and has setup policy framework, issued guidelines and regulatory mandates for secure implementation and management.



Regulation in effect in India	Focus Area
<b>The Indian Telegraph Act and Rules<sup>29</sup></b>	<ul style="list-style-type: none"> <li>• Prohibits and penalizes unlawful interception of communication and tampering with messages sent over telegraphs</li> <li>• Licenses issued to Telecom Service Providers (TSPs) under this Act require TSPs to take measures to safeguard the privacy of their customers and confidentiality of communications</li> </ul>
<b>Telecom Regulatory Authority of India (TRAI)<sup>30</sup></b>	<ul style="list-style-type: none"> <li>• Issued a direction seeking to implement the privacy and confidentiality related clauses in the service providers' licenses</li> <li>• Service providers are required to put in place an appropriate mechanism to prevent the breach of confidentiality on information belonging to the subscribers and privacy of communication</li> </ul>
<b>Department of Telecom (DoT)<sup>31</sup></b>	<ul style="list-style-type: none"> <li>• Includes the security conditions in the UASL that are to be adhered to by the telecom service providers</li> <li>• Mandates in UASL to induct only those network elements which have been tested as per relevant contemporary Indian or International Security Standards and certified by authorized and certified agencies/ labs in India</li> </ul>
<b>National Telecom Policy 2012<sup>32</sup></b>	<ul style="list-style-type: none"> <li>• Provides directions to build national capacity in all areas - specifically security standards, security testing, interception and monitoring capabilities and manufacturing of critical telecom equipment</li> <li>• Mandates and enforces that the Telecom Service Providers take adequate measures to ensure the security of the communication flowing through their network by adopting contemporary information security</li> </ul>
<b>IT Amendment Act 2008 (ITAA 2008)<sup>33</sup></b>	<ul style="list-style-type: none"> <li>• Mandates implementation of reasonable security practices and procedures with respect to Sensitive Personal Information of any individual</li> <li>• Has provisions to penalize on fraudulent use of identity of an individual and criminalizes wrongful disclosure of personal information in breach of lawful contract</li> </ul>
<b>Amendment to the Unified Access Service license agreement 2011<sup>34</sup></b>	<ul style="list-style-type: none"> <li>• Includes requirements such as existence of organizational Information Security Policy covering Security Management, Network Forensics &amp; Hardening, conduct of Network penetration testing, Risk assessment, establishment of security operations center (SOC), etc.</li> </ul>
<b>National Cyber Security Policy, 2013 (NCSP-2013)<sup>35</sup></b>	<ul style="list-style-type: none"> <li>• The mission is to protect information and information infrastructure in cyber space, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities, and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation</li> <li>• Aims at facilitating creation of secure computing environment and enabling adequate trust and confidence in electronic transactions and also guiding stakeholders' actions for protection of cyber space</li> <li>• Aims at creating a secure cyber ecosystem and an assurance framework, encouraging open standards, strengthening the regulatory framework, vulnerability management, promotion of research and development in cyber security and enhancing our technical skill sets and human resources</li> </ul>



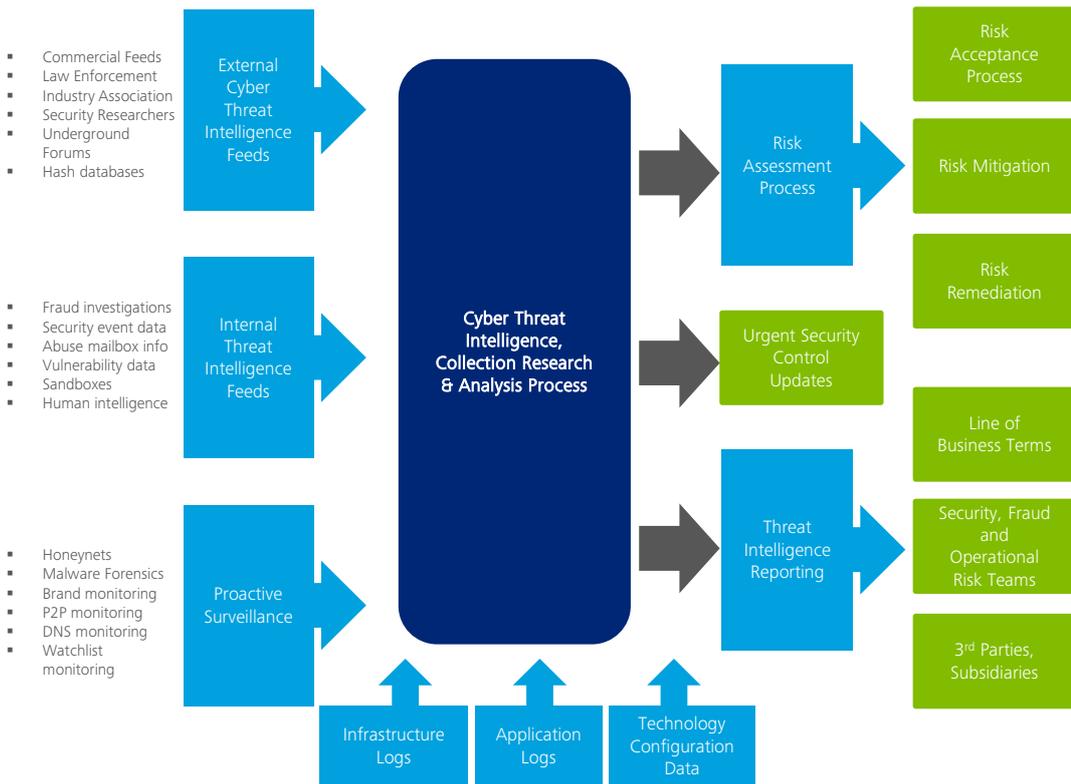
### The middle way

In spite of a slew of regulations, telecom remains one of the most attacked sectors in India by cyber criminals. Though these regulations are intended to create a robust security and compliance environment, many regulations fall short of meeting their intended purpose. While several reasons can be attributed to this failure, it is imperative to take cognizance of such failures and work towards building a balanced approach to deal with ever evolving landscape of cyber threats.

### Building 'actionable' cyber threat intelligence<sup>36</sup>

Competition, customer demand, and technological advances in mobile technologies lure telecom service providers to focus more on innovative business models and not giving cyber security its due importance. Most of the times, cyber security is considered as an afterthought.

Figure 5: Cyber intelligence acquisition and analysis



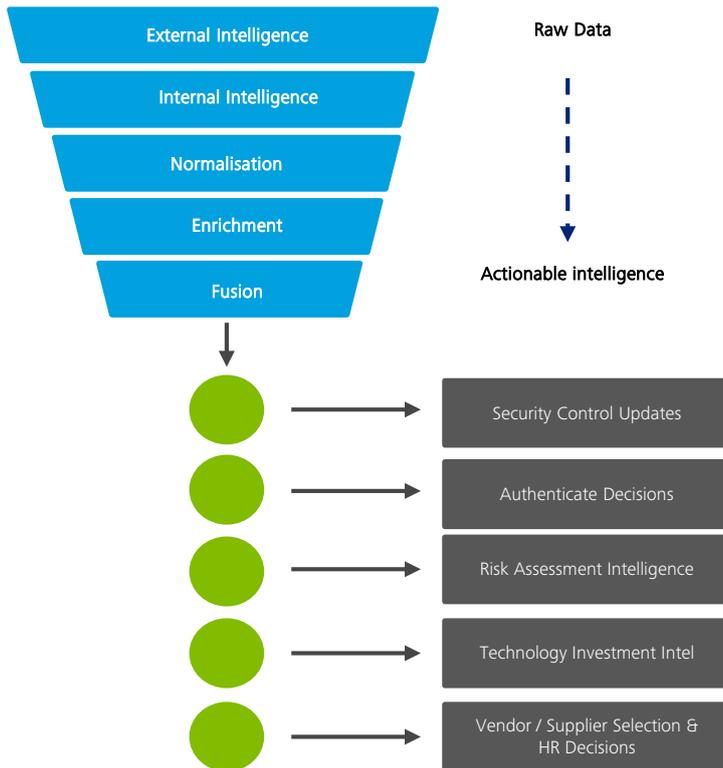
Telecom companies should consider integrating cyber security as a key component in their business models so that customer demands can be met without compromising on security.

They should identify, at a high level, the complete range of players and the information resources in use by both their own organization and processing partners as many sensitive items may be outside the organization's perimeter, yet still within the business's responsibility. This work is best organized around business processes rather than by organization or technology platform, so follow the information process.

While organizations focus a lot on having robust enterprise architecture, information security still comes as an afterthought. Gone are the days when information used to stay within the boundaries of the data centers. In the modern environment of mobility, information is available on the fingertip through various smart devices and platforms.



Figure 6: The new approach for cybersecurity – Proactive<sup>37</sup>



It is imperative that telecom organizations revise/ realign their security strategy and IT architecture to ensure that there exists a robust security architecture which adopts a data-centric rather than data center approach. Security architecture must enable the organization to become cyber-risk intelligent and resilient.

**A forward looking cyber threat intelligence capability**

- Conduct emerging threat research
- Establish partnership to share intelligence
- Assign threat focus areas
- Establish live, dynamic intelligence feeds
- Implement a holistic approach to cyber threat identification
- Actively track the cyber-criminal elements
- Perform daily emerging threat reviews
- Maintain awareness of the changing technology and business environment
- Patch operating system, network, process and application vulnerabilities
- Deploy and maintain signature and behavior based controls
- Produce metrics and trending data for multiple key threat indicators
- Continuously improve automation capabilities



### **Building capacity and capability**

While there is a rapid surge in cyber-attacks, the country is scouting for the right cyber skills and talent. It is estimated that there is a serious dearth of cyber security professionals in the country and India will need 1 million trained cyber security professionals by 2020.<sup>38</sup>

There is an immediate need to have a PPP model for increasing the security awareness among the users of the ICT. In addition, an initiative for providing the cybersecurity training under the *Skill India* program may be taken to backfill the shortage of professionals trained on various aspects of cybersecurity. The bodies such as ISACA (India chapter), DSCI, Cert-In, etc. should come together and with the support from the private organizations should cater to this requirement.

### **Security assessment and testing**

The network elements and related infrastructure require undergoing a holistic security assessment and penetration testing program. With the rollout of 4G, a large volume of network components are now IP-enabled: this brings all IP-related vulnerabilities in the telecom network that otherwise would be available on only general IT systems. Therefore, it is imperative to carry out a regular security testing that should include vulnerability assessment and penetration testing of these components. In addition, a thorough risk assessment must be carried out for all the processes that are enabled through these network components. A holistic end-to-end security assessment and testing program should be developed and implemented. Where possible, a security baseline for each type/ category of network elements should be created. The outcome of such assessments/ testing may be reported to stakeholders for providing an assurance.

### **Enriched coordination**

In the current scenario, there is a lack of alignment within various government bodies that are dealing with cyber security and private organizations that are putting in place their own set of policies, processes, security infrastructure, etc. There is a need to move away from working in silos and have coordinated efforts to combat cyber-threats.

The Government of India has formed the National Critical Information Infrastructure Protection Centre (NCIIPC) to act as the primary body for safeguarding the critical information infrastructure in the country.<sup>39</sup> NCIIPC has been directed to work under the guidance of National Technical Research Organization (NTRO). The NCIIPC may act as a central body responsible for bringing all the interested and impacted parties together to form a consortium/ body to devise a collaborative strategy and plan to deal with cybercrimes and associated risks. This body/consortium may act to resolve any duplicity, redundancy and/ or conflicts between various regulatory requirements, Acts, conditions, etc. that relate to cybersecurity and hinder their implementation.

The body/ consortium should consider the future of cybersecurity in the form of sustainable risk management. The tipping point of cyber will likely come when it blends seamlessly with the organization's broader business portfolio and becomes part of how it operates and delivers on its mission. It calls for a new cultural approach that's integrated into almost every aspect of public and private life. People will compare trade-offs and make tough choices based on data from a real-time view of the cyber landscape. It will take some funding but equally important to creating an effective cyber deterrence strategy is dedicated leadership, public and private sector collaboration, and the commitment of citizens.

# Evolving Technology: Can India afford to be left behind?



The telecom industry around the world is redefining communication services more frequently than ever. The bandwidth promised by newer technologies is setting new benchmarks rapidly. Every new technology is superior to the former one by 100 or even 1000 times. The way people communicate changed over time from cave paintings and carrier pigeons to instant messaging, M2M, and augmented reality. Now communication technology has the ability to catalyze the process of economic growth and development of a country.

## The story so far

The process for faster communication in India started in 1881 with telephone exchanges in Calcutta, Mumbai, and Chennai. There has been a remarkable growth in the telecom market since the privatization of the sector in 1990. However, India has been lagging behind the other developing and developed countries in terms of technology adoption. Technology adoption is slow on both demand and supply side (i.e. among the customers as well as the operators). The 2G technology, released worldwide in the year 1991, was commercially introduced in India in the year 1995. Similarly, 3G technology was first commercially launched in Japan in 2001 while the 3G spectrum auction in India took place in 2010. The 4G technology is now being launched by a few players across the country.

The Indian communication sector has witnessed tremendous growth in the last two decades. The growth is not only in terms of subscriber base but also in terms of mobile users, smartphones, voice and data based services. The technology has also evolved over the years to provide better voice and data services to a large number of subscribers in a limited spectrum range.

The post liberalization era (i.e. 1990-1999) has changed the face of the Indian telecom sector by some major policy changes and privatization of the sector. The Indian telecom sector is now the 2nd largest market in the world with more than a billion subscribers. The privatization of the industry and 100% FDI permission in the sector attracted many international investors and operators to the country. The private players boast almost 90% of the wireless market share. The teledensity has increased to 79.38.<sup>40</sup> There is almost 12% annual growth in the data subscribers which is higher than that in the US and China with annual growth of 7% and 4%, respectively. While the data services are the new frontier for growth in urban areas, voice services still have potential in rural and remote areas.

Despite the launch of 3G services in 2010, there is less than 10% 3G penetration in India. The basic phones still command 70% of the mobile shipments in India. Out of the 77 million smartphones shipped in India, only 73% were 3G capable.<sup>41</sup> Nevertheless, the 3G adoption has picked up in 2013 and 2014 showing growth of 114% during that period.<sup>42</sup> Like 3G, the case of 4G has also not been meaningful so far. It has been 5 years since operators won the spectrum for launching 4G services in India in 2010, but the rollout is delayed. Only a few operators have managed to launch 4G services significantly in bigger cities. While many of the developed and developing countries have done 100% 4G rollout, India is lagging behind.

Of the 550,000 telecom towers in India, only 165,000 are 3G-enabled. Globally, most countries have over 70% 3G-compatible towers. It took an average of 3 years to develop a full-fledged 3G network in most countries while even after 5 years of auction, the 3G service in India lacks reachability and the desired speed. Customers still prefer 2G services not only for low tariffs but also since they do not see any difference in 3G and 2G data speed in India. Moreover, 3G network doesn't have consistent coverage across the country. Currently, around 14% of all calls get dropped which is 7 times higher than acceptable limit of 2%.

			
<b>Total subscribers</b>	329 million	1.29 billion	1 billion
<b>3G Launch</b>	2008	2008	2010
<b>3G subscribers</b>	225 million	695 million	82 million
<b>4G Launch</b>	2010	2010	2012
<b>4G subscribers</b>	100 million	250 million	85000

### The case of 5G

The world is slowly moving towards the 5G technology while India is struggling to adopt 3G/4G. The large scale shift from 2G to 3G and 4G is yet to happen. The wireless industry showcased the idea for 5G technology in the Mobile World Congress 2015 and is expected to commercially launch by 2020. Researchers at the University of Surrey, UK and University of Sydney, Australia managed to record an incredible 1 Tbps speed during a test, and this service is around 65,000 times faster than current 4G speeds.

The 5G technology can bring a paradigm shift in the wireless networks with new features like:

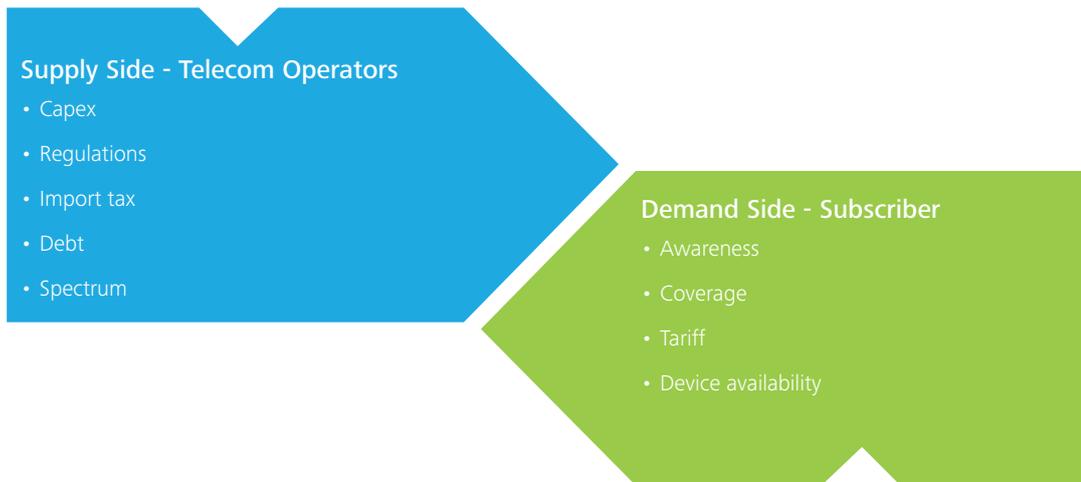
- Faster speed of up to 10 Gbps
- Reduced latency of 1 milli-sec, 500 times faster than current LTE technologies
- Green and sustainable infrastructure
- Flexibility enabling different wireless technologies to coexist and share resources
- Highly secure network offering seamless and uninterrupted connectivity

### Challenges for telecom operators

There are many factors that drive the technology adoption from both demand and supply side. Lack of technology ecosystem, relevant content and services, low-cost 4G enabled handsets, delayed government processes like right of way and permissions, etc., are causing the delay in the launch of 4G services and greater penetration of 3G. Some other challenges for operators in India are low ARPU, high investment in spectrum and infrastructure, low tariff, and a highly competitive market.



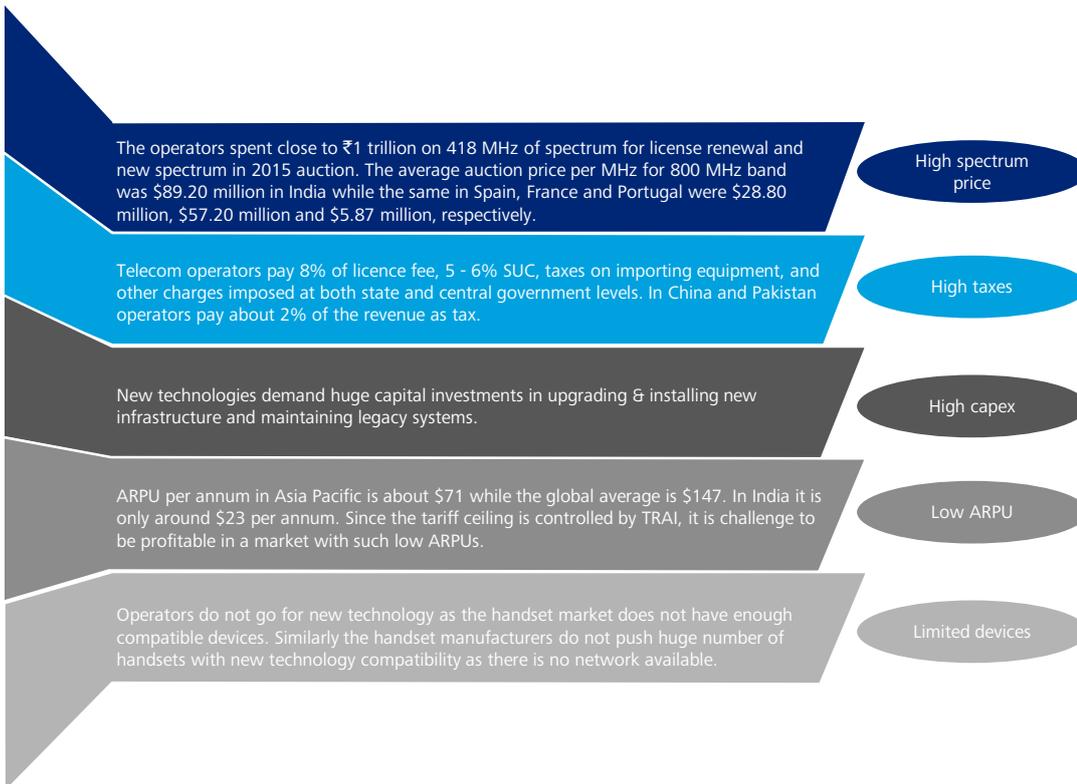
Figure 7: Drivers of technology adoption



The saturating wireless voice market is leading to a decline in net subscriber additions in India, adversely affecting voice services revenue growth. Wireline subscribers are estimated to fall 7% YoY to 26.59 million at end of March 2015 as consumers shift to wireless services. New market entrants in the telecom and technology space like VOIP and messenger service providers change business rules and revenue streams are increasingly less predictable.

Network upgrade and maintenance costs continue to escalate due to mounting data traffic, forcing operators to optimize network utilization. After the spectrum auction 2015 the combined debt of Indian telecom players increased to ₹3.5 trillion post payment of spectrum price.<sup>43</sup>

Figure 8: Challenges faced by telecom operators in India



The combined effect of all these challenges does not allow telecom operators to deploy new technologies faster. In addition, regulatory issues such as strict radiation norms, rollout obligations, etc., hit core service areas. Incumbents feel government and stakeholder pressure to service currently uncovered areas.

However, intensifying competition, slowing revenue growth, and increasing network costs would compel telecom operators to deploy advanced technology solutions. These solutions could help them reduce churn by offering personalized services and innovative price plans, which could attract positive customer reviews, in turn drawing new customers. Increased automation and proper network management with Self-Organising Network (SON), predictive operations can help in better management of calls and signal strength. To cater to large traffic volumes expected in next 4-5 years, operators are expected to off-load a large amount of traffic on micro sites, small cells, and Wi-Fi, which might render the macro site tenancy growth lesser than expected. Tower companies in developed markets derive a significant portion of their revenues from small cell network solutions e.g. ATC generates about 2-3% of its revenue and Crown Castle generates about 7% of its revenue through small cell offerings.

Based on the above, the return on investment in these technologies may not be clear and that may perhaps be the reason for delay in technology adoption. They are also concerned about the high cost of implementing analytics solutions and deploying new infrastructure in a vast country, collecting data from several departments, and integrating data and equipment from legacy and next-gen infrastructure systems. Telecom companies also often lack the talent required to fully leverage the power of newer technologies.

However, operators could get too focused on the short term and develop a myopic vision. Hence there is a need to balance short and long-term goals.



## Ways to encourage technology adoption

### Operators

- **Competitive advantage:** New technology adoption could provide a competitive advantage in the saturated and highly competitive Indian market. The huge population and mostly untapped rural market shows tremendous potential. Though technology diffusion is slow in India, the significance of new technology is high, looking at the high potential of the market.
- **New revenue stream:** The adoption of new technology can provide the much required new revenue streams. The rise of data-based services like Internet of Things, e-commerce and social networking have started generating huge data traffic. These open up new business opportunities such as analytics, cloud, wearables which they can monetize upon the user data. New technology adoption can help in providing vertical services such as m-banking, e-health and e-education and help in differentiating their service provision in highly commoditized telecom market.
- **Improve service offerings:** Analytics solutions could help in reducing network costs and retaining customers as it helps in improving data traffic management and optimizing the utilization and performance of networks. New technology solutions could help in reducing churn by offering personalized services and innovative price plans, which could attract positive customer reviews, in turn drawing new customers.
- **Awareness:** Lack of awareness is one of the primary reasons for low technology adoption in India. Increasing awareness of services such as m-banking and m-payments could help in greater technology adoption from the customer side. The efficiency and reach of government services like m-Gov/e-governance and other digital services related to agriculture, health and education could attract consumers in urban as well as rural areas. Government, social networks, media can help in increasing awareness of customers and encourage them to use new technologies to access different services by clearly demonstrating the benefits promised by these technologies.

### Government

There are various ways in which the government can help in faster technology adoption in the country. Liberal policies on tax and light touch regulations would go a long way in attracting more investments in technology development in India. The broadband highway, Digital India and 100 smart cities projects are encouraging technology innovation in India. Other initiatives of the government that have gathered positive response from Industry, investors, startups and consumers are the following:

- **Make in India:** The Make in India initiative will greatly help the domestic equipment manufacturers. India's imports of telecom equipment in FY14 was ₹69.51 billion against exports of ₹20.48 billion, resulting in a net foreign exchange outgo of ₹49.04 billion.<sup>44</sup> Liberal regulations and tax policies can encourage domestic and international players to make in India and hence open their R&D centers locally. This will directly impact the technology innovation as well as adoption in India with inherent benefits from local taxes and reduced / no customs duty.
- **Spectrum sharing:** Recently government has allowed the telecom operators to share spectrum for efficient and optimum utilization of the limited natural resource. Mobile operators in India have only about a third of the spectrum compared to global operators to serve the 2nd largest market in the world. Though spectrum sharing is permitted, the policies need to be more liberal to reap full benefits of the spectrum sharing model. Restriction on inter-band sharing limits the opportunity as an operator cannot share extra spectrum with other operator who do not have spectrum in the same spectrum band.<sup>46</sup> Limitations on sharing of liberalized and un-liberalized spectrum (acquired administratively) are also discouraging for operators. Apart from these, government needs to free additional spectrum in more efficient spectrum bands like 700 MHz. This will not only help in improving the network coverage but also help the operators in lower capital expenditures as lesser BTS systems are required in lower frequency bands.



### Concluding remarks

India is lagging behind the world in technology adoption, and this may get aggravated if we do not leapfrog to future technologies. India is currently seeing the growth of 3G services, and we are hopeful of the success of 4G services in the future. We may see the leapfrogging of 2G users to 4G instead of the natural linear progression from 2G to 3G to 4G. Mainstream adoption of 4G may see negative growth in 3G subscribers too. In South Korea, the net 3G subscriber addition turned negative immediately after the launch of 4G. Similar trends were seen in Japan.

To remain relevant in the fast-paced digital world, operators need to embrace latest technologies at faster rate and make them available for end users. Telecom operators will need to have long-term vision and discover innovative business models collaborating and co-operating with each other leading to win-win situation for all players in the value chain. This can only be achieved with timely and appropriate regulatory support from the government with light touch regulations, funding support and liberal tax reforms to encourage domestic and international players. We will need another paradigm shift in the telecom market to raise the bandwidth from current unacceptable levels of few kbps in India to the global benchmarks of several Mbps. In the digital era, providing better connectivity and device availability at low cost for the masses and classes in India could go a long way in the growth and prosperity of the country.

# About Confederation of Indian Industry



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 organization, playing a proactive role in India's development process. Founded in 1895, India's premier business association has over 7900 members, from the private as well as public sectors, including SMEs and MNCs, and an indirect membership of over 200,000 enterprises from around 240 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 specialized 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 organizations 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.

In its 120th year of service to the nation, the CII theme of **"Build India- Invest in Development, A Shared Responsibility"**, reiterates Industry's role and responsibility as a partner in national development. The focus is on four key enablers: Facilitating Growth and Competitiveness, Promoting Infrastructure Investments, Developing Human Capital, and Encouraging Social Development.

With 66 offices, including 9 Centres of Excellence, in India, and 8 overseas offices in Australia, Bahrain, China, Egypt, France, Singapore, UK, and USA, as well as institutional partnerships with 312 counterpart organizations in 106 countries, CII serves as a reference point for Indian industry and the international business community.



# Acknowledgements

**Shree Parthasarathy**

Senior Director

**P.N. Sudarshan**

Senior Director

**Gaurav Shukla**

Director

**Vivek Jhunjhunwala**

Manager

**Anu Peisker**

Manager

**Raja Ramesh**

Deputy Manager

**Deepak Sidha**

Executive Officer  
Confederation of Indian Industry

## Contacts

---

**Confederation of Indian Industry**

(Northern Region) – Sub-Regional Office  
Plot No 249 –F, Sector-18, Udyog Vihar  
Phase IV, Gurgaon - 122 015  
Telephone: 91-124-4014073 / 4014060-7  
Fax: 91 124 4014070  
e-mail: [ciinr@cii.in](mailto:ciinr@cii.in)  
Website: [www.cii.in](http://www.cii.in)

**Deloitte**

7th Floor, Building 10, Tower B,  
DLF Cyber City Complex, DLF City Phase - II  
Gurgaon - 122 002, India  
Telephone: +91-0-124 679 2000  
e-mail: [inideas-tmt@deloitte.com](mailto:inideas-tmt@deloitte.com)  
Website: [www.deloitte.com/in](http://www.deloitte.com/in)

# References



- <sup>1</sup> VNI Mobile Forecast Highlights, 2014 – 2019, Cisco. See: [http://www.cisco.com/assets/sol/sp/vni/forecast\\_highlights\\_mobile/index.html#~Country](http://www.cisco.com/assets/sol/sp/vni/forecast_highlights_mobile/index.html#~Country)
- <sup>2</sup> <http://www.hindustantimes.com/advertorial/digitizing-india-changing-the-face-of-connected-living/article1-1359806.aspx>
- <sup>3</sup> Prime Minister Narendra Modi announces Centre of Excellence for IoT, July 2015, NASSCOM Press Release. See: <http://www.nasscom.in/prime-minister-narendra-modi-announces-centre-excellence-iot-partnership-nasscom-deity-and-ernet>
- <sup>4</sup> <http://economictimes.indiatimes.com/cisco>
- <sup>5</sup> Get Ready for the Next Generation of Smart Products, Feb 2015. See: <http://www.cmswire.com/cms/internet-of-things/get-ready-for-the-next-generation-of-smart-products-027957.php>
- <sup>6</sup> Internet of Everything (IoE) Top 10 Insights from Cisco's IoE Value Index Survey. See: <https://cloudwiser.wordpress.com/2014/02/11/internet-of-everything-ioe-top-10-insights-from-ciscos-ioe-value-index-survey-of-7500-decision-makers-across-12-countries/>
- <sup>7</sup> The more things change: Value creation, value capture, and the Internet of Things, Michael E. Raynor & Mark J. Cotteleer, Deloitte Review, Issue 17. See: <http://dupress.com/periodical/deloitte-review/issue-17/>
- <sup>8</sup> The internet of things in Japan: See: <http://www.huawei.com/en/about-huawei/publications/winwin-magazine/hw-110837.htm>
- <sup>9</sup> GSMA Report. See: <http://www.gsma.com/newsroom/press-release/china-global-leader-ideployment-internet-of-things-finds-new-gsma-report/>
- <sup>10</sup> The Alliance for Internet of Things Innovation (AIOTI). See: <https://ec.europa.eu/digital-agenda/en/alliance-internet-things-innovation-aioti>
- <sup>11</sup> IoT and the Smart Nation. See: <https://www.ida.gov.sg/Tech-Scene-News/Tech-News/Smart-Nation/2015/6/IoT-and-the-Smart-Nation>
- <sup>12</sup> Ambient computing: Putting the Internet of Things to work, Tech Trends 2015, Deloitte. See: <http://www2.deloitte.com/global/en/pages/technology/articles/tech-trends.html>
- <sup>13</sup> Net Neutrality as Global Principle for Internet Governance, IGP, November 2007. See: <http://internetgovernance.org>
- <sup>14</sup> Tech Bytes: TMT sensing widget, Edition 6, May 2015, Deloitte Australia
- <sup>15</sup> Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2014–2019 White Paper, Feb 2015. See: [http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white\\_paper\\_c11-520862.html](http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html)
- <sup>16</sup> Internet traffic in India grew 74% in 2014, Feb 2015, TOI. See: <http://timesofindia.indiatimes.com/tech/tech-news/Internet-traffic-in-India-grew-74-in-2014/articleshow/46287859.cms>
- <sup>17</sup> E-Commerce in India – Past, Present & Future: See more at: <http://www.iamwire.com/2014/07/e-commerce-in-india-past-present-future/27805>
- <sup>18</sup> E-Commerce Industry In India Worth \$13.5 Billion In 2014, March 2015. See: <http://dazeinfo.com/2015/03/19/e-commerce-industry-india-worth-13-5-billion-2014-will-cross-16-billion-2015/>
- <sup>19</sup> 100 million online shoppers in India by 2016: Report: See <http://www.livemint.com/Industry/nWCyKyN5fleBTDQPU5AwM/100-million-online-shoppers-in-India-by-2016-Report.html>
- <sup>20</sup> Global Retail E-Commerce Keeps On Clicking, See more at: [https://www.atkearney.com/consumer-products-retail/e-commerce-index/full-report/-/asset\\_publisher/87xbENNHPZ3D/content/global-retail-e-commerce-keeps-on-clicking/101927\\_101\\_INSTANCE\\_87xbENNHPZ3D\\_redirect=%2Fconsumer-products-retail%2Fe-commerce-index](https://www.atkearney.com/consumer-products-retail/e-commerce-index/full-report/-/asset_publisher/87xbENNHPZ3D/content/global-retail-e-commerce-keeps-on-clicking/101927_101_INSTANCE_87xbENNHPZ3D_redirect=%2Fconsumer-products-retail%2Fe-commerce-index)
- <sup>21</sup> IBEF Report See more at: <http://www.ibef.org/industry/indian-consumer-market.aspx>
- <sup>22</sup> TRAI performance indicator report. See more at: <http://www.trai.gov.in/WriteReadData/PIRReport/Documents/Indicator-Reports-Mar12082015.pdf>
- <sup>23</sup> Deloitte study on “Global Powers of Retailing 2015: Embracing innovation”. See: <http://www2.deloitte.com/global/en/pages/consumer-business/articles/global-powers-of-retailing.html>
- <sup>24</sup> 41% of India E-commerce sales is from Mobile; Mobile wallet usage surging: Meeker's 2015 Internet Trends. See: <http://tech.economictimes.indiatimes.com/news/internet/41-of-india-e-commerce-sales-is-from-mobile-mobile-wallet-usage-surging-meekers-2015-internet-trends/47452981>
- <sup>25</sup> India sees more cashless transactions through internet, ATM, etc. as consumers favour virtual payment. See: [http://articles.economictimes.indiatimes.com/2015-05-25/news/62624723\\_1\\_transactions-lakh-core-payment-bank-licence](http://articles.economictimes.indiatimes.com/2015-05-25/news/62624723_1_transactions-lakh-core-payment-bank-licence)
- <sup>26</sup> IBEF Report See more at: <http://www.ibef.org/industry/retail-india.aspx>
- <sup>27</sup> Deloitte Cyber Threat Intelligence. See: [http://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/ZA\\_RA\\_CyberCrime\\_CombatingFastestGrowingCyberSecurityThreat\\_2015.pdf](http://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/ZA_RA_CyberCrime_CombatingFastestGrowingCyberSecurityThreat_2015.pdf)
- <sup>28</sup> Deloitte 2013 TMT Global Security Study. See: <http://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/2013-tmt-global-securitystudy.html>
- <sup>29</sup> <http://www.dot.gov.in/act-and-rules/indian-telegraph-act>
- <sup>30</sup> <http://www.trai.gov.in/WriteReadData/Direction/Document/Direction3dec10.pdf>
- <sup>31</sup> [http://www.dot.gov.in/sites/default/files/as-iii\\_2.pdf](http://www.dot.gov.in/sites/default/files/as-iii_2.pdf)
- <sup>32</sup> [www.trai.gov.in/WriteReadData/userfiles/file/NTP%202012.pdf](http://www.trai.gov.in/WriteReadData/userfiles/file/NTP%202012.pdf)
- <sup>33</sup> [http://deity.gov.in/sites/upload\\_files/dit/files/downloads/itact2000/it\\_amendment\\_act2008.pdf](http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf)
- <sup>34</sup> [http://www.dot.gov.in/whats-new/amendment-unified-access-service-licence-agreement-security-related-concerns-or-expansion-](http://www.dot.gov.in/whats-new/amendment-unified-access-service-licence-agreement-security-related-concerns-or-expansion)
- <sup>35</sup> [http://deity.gov.in/sites/upload\\_files/dit/files/National%20Cyber%20Security%20Policy%20\(1\).pdf](http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf)
- <sup>36</sup> Cybercrime: a clear and present danger, Deloitte. See: [http://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/ZA\\_RA\\_CyberCrime\\_CombatingFastestGrowingCyberSecurityThreat\\_2015.pdf](http://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/ZA_RA_CyberCrime_CombatingFastestGrowingCyberSecurityThreat_2015.pdf)
- <sup>37</sup> Cyber Espionage, Deloitte
- <sup>38</sup> Cyber Security: 1 million cyber security professionals needed by 2020. See: [http://articles.economictimes.indiatimes.com/2015-08-25/news/65847438\\_1\\_cyber-security-ethical-hacking-information-security](http://articles.economictimes.indiatimes.com/2015-08-25/news/65847438_1_cyber-security-ethical-hacking-information-security)
- <sup>39</sup> National Critical Information Infrastructure Protection Centre (NCIIPC). See: <http://indiasmartgrid.org/en/Lists/Member/Attachments/19/ISGD%20Plenary%20III%20Muktesh%20Chander%20NCIIPC.pdf>
- <sup>40</sup> TRAI performance indicator report. See: <http://www.trai.gov.in/WriteReadData/PIRReport/Documents/Indicator-Reports-Mar12082015.pdf>
- <sup>41</sup> Distress Call. See: <http://www.businesstoday.in/magazine/trends/factors-that-are-contributing-to-death-of-3g-in-india/story/220551.html>
- <sup>42</sup> Indian telecom industry: Looking beyond 3G and 4G: See: <http://telecom.economictimes.indiatimes.com/tele-talk/Indian-telecom-industry-Looking-beyond-3G-and-4G/828>
- <sup>43</sup> Payment may push telcos' debt to Rs 3.5 lakh cr, See: <http://www.financialexpress.com/article/economy/payment-may-push-telcos-debt-to-rs-3-5-lakh-cr/57788/>
- <sup>44</sup> Telecom department bets on 'Make In India' to cut equipment imports: See: <http://www.dnaindia.com/money/report-telecom-department-bets-on-make-in-india-to-cut-equipment-imports-2058478>
- <sup>45</sup> Approval to guidelines on spectrum sharing, Government of India Press Release, August 2015. See: <http://pib.nic.in/newsite/PrintRelease.aspx?relid=124945>
- <sup>46</sup> Distress Call, See: <http://www.businesstoday.in/magazine/trends/factors-that-are-contributing-to-death-of-3g-in-india/story/220551.html>

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms

This material and the information contained herein prepared by Deloitte Touche Tohmatsu India Private Limited (DTTIPL) in association with Confederation of Indian Industry (CII) and is intended to provide general information on a particular subject or subjects and is not an exhaustive treatment of such subject(s). None of DTTIPL, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is and CII, by means of this material, rendering professional advice or services. The information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network and at CII shall be responsible for any loss whatsoever sustained by any person who relies on this material.  
© 2015 Deloitte Touche Tohmatsu India Private Limited. Confederation of Indian Industry (CII)