Deloitte.

Confederation of Indian Industry
125 Years - Since 1895

Internet of Things (IoT)

The rise of the connected world

Contents

Foreword from CII

Dr. Rishi Bhatnagar
Summit Chairman and
President, Aeris Communications India

The age of connected technologies and Internet of Things has now arrived!

COVID-19, the novel coronavirus, brought the whole world in the eye of the storm, and has driven organisations to rethink the way they work and operate. Many employees have been told to work from home, and use videoconferencing and online collaboration services. The effects of the pandemic on the global economic recession are causing CIOs to prioritise spending on technology and services that are deemed "mission-critical" over initiatives aimed at growth or transformation. Investing in connected technologies is no more a luxury, but a necessity for survival and business continuity.

While we were already witnessing enterprises investing in conducting proof of concepts and smaller implementations of connected technologies as a huge incentive to improve efficiencies and reduce downtime, mass adoption rates were never quite impressive. The pandemic is leading to global business shutdowns, supply chain disruptions, social distancing, and remoting working (a new normal). We are registering a huge surge in the number of deployments, especially in the enterprise and automotive sectors. In these sectors, the Internet of Things (IoT) market is projected to grow to 5.8 billion endpoints in 2020, up from 21 percent in 2019, as predicted by one of the leading analyst firms.

The market for IoT will improve further as this technology provides businesses and people better insights into and control on objects and environments that remain beyond the reach of internet. And by doing this, IoT allows businesses and people to be more connected to the world around them and do more meaningful, higher-level work. Improvements in the last-mile connectivity, cheaper sensors, availability of low power technology, and long-lasting batteries are making IoT solutions more relevant and affordable compared with the situation a decade ago.

IoT is disrupting both the consumer (retail, healthcare, and services) and industrial sectors, such as transportation, water, oil and gas, agriculture, and manufacturing. In the manufacturing sector, the business of extracting and transporting oil and gas is filled with challenges. To stay competitive, companies must continually strive to produce crude oil and refined products at a lower cost. Manufacturers are adopting IoT with the increased use of robotics, sensors, cloud, centralised tracking, quality inspection, etc., forming an "ecosystem" of smart manufacturing. Similarly, power suppliers and utility companies are finding IoT technologies promising to drive internal and external benefits and achieve success as they develop programmes that encourage their customers to participate. Precision in **water irrigation systems** with IoT sensors, including trickle and subsurface methods, greatly reduces water consumption. These systems have the ability to integrate with utility demand response systems. Demand response programmes help reduce peak demand during periods of limited electrical supply in the grid.

The IoT cloud platform market is expected to grow from US$ 6.4 billion in 2020 to USD$ 11.5 billion by 2025. The IoT solution segment has dominated the overall **IoT monetisation market**. It is expected to continue this trend due to increasing adoption of IoT monetisation solutions among organisations, as they are finding ways to monetise IoT through revenue-generating products and services or differentiate their core product and service offerings with innovative business models.

With data orchestration deployments, IoT is growing organically right now, from devices and up. IoT orchestration offers the ability to integrate IoT with existing business workflows and systems. It also provides a single platform that unifies data from current and future connected devices and systems.

Unlocking value from any technology requires more than blind investments. Organisations most likely to pull ahead of their competitors will be the ones that focus on security, performance, and standard implementation to drive success, as well as get their customers on board early. Whether it is the consumer IoT and the industrial IoT, IoT adopters must look beyond the "wow" factor to ensure that they are getting IoT solutions designed for their needs.

Moreover, IoT devices are becoming a matter of increasing concern in terms of data privacy and cybersecurity aspects. Although emerging devices are easily identified at inception, decades-old technology has become part of the IoT universe–sometimes stealthily–and must be dealt with. These devices must be properly segmented and managed from a policy perspective because they are a gateway to an organisation's broader, connected infrastructure. Emerging IoT devices are likely to be built and deployed with security in mind. However, more familiar hardware that now has intelligence and connectivity might get overlooked. With India announcing its data privacy laws soon, our systems will become more secure and robust.

Foreword from Deloitte

Ashvin Vellody
Partner, Deloitte Touche Tohmatsu India LLP

Technology is playing a pivotal role in helping societies respond, recover, and thrive in the COVID-hit world. The increasing importance of capturing real-time data and acting upon the insights is driving focus on Internet of Things (IoT) – both in terms of its wider applicability and the path towards achieving scale. IoT software spending totalled US$39.3 billion in 2019 in APAC region. It is expected to increase rapidly at a CAGR of 14.4 percent over the five-year forecast period (2018-23). This increase is fuelled by ever-declining cost of computing power, advancement in efficient algorithm designs, progress in machine learning, and above all, the rise of low latency, high-range networks. These networks will become even more pervasive after the wider adoption of 5G networks in different regions of the world.

For businesses across the globe, IoT has passed the stage of being seen only as an exploratory technology. Numerous use cases exist for most industry sectors where IoT, along with other exponential technologies, is driving operational efficiencies, newer business models, and smarter and sustainable communities. While economic and technological barriers are receding, significant obstacles are hindering the adoption of IoT. Executives are worried about security, interoperability, and privacy elements; standards and regulations put in place to address these challenges would help the overall ecosystem.

We are still in the early stages of adopting IoT in India. While a wide range of sectors are going through slump, analysts, investors, IoT technology providers, and enterprises believe we are on the cusp of an explosion in the wider adoption of IoT. With the proliferation of connected devices and evolving artificial intelligence (AI) capabilities, the applicability of IoT is set to expand for businesses, consumers, and citizens. The agriculture industry is already experimenting with more efficient irrigation and soil monitoring. The healthcare and wellness industry is developing innovative applications with wearables for remote monitoring, disease prediction, and diagnosis. Watch out for unicorns in this space!

As machines become more intelligent, this technology can have a positive impact on the everyday lives of citizens. This report aims to provide an industry overview and has covered the impact of COVID-19 on IoT. It starts by identifying a market structure, followed by a discussion on the challenges the industry is facing with respect to IoT adoption and opportunities that adopters can exploit. The report also covers a few sectors that are early adopters of IoT and highlights how their business is changing. It looks at key industry players to know how they are evolving in the current IoT age. New business models and offerings that players could come up with are also being discussed. Finally, given the concerns around data security and privacy, we have dedicated an entire section to share our perspectives.

We hope you find this report insightful and enriching. Let the conversations begin...

Happy reading!

Introduction

Technology is shaping the world like never before. The government and business leaders in India must harness the opportunities offered by technology and its implications on the future of work.

COVID-19 and the resulting geopolitical fall out have made it more urgent for corporate leaders to ensure that India is able to respond to the new normal. They also need to ensure that the country can seize the opportunity to increase its market share in the global manufacturing economy.

COVID-19 has precipitated companies' entire focus towards industry 4.0. Two things that have become more important for companies today are: focusing on adopting digital technologies that constitute the Industrial 4.0 revolution, and investing in new products and services that enable them to thrive in the fast-evolving economic environment.

This report discusses why we believe IoT, the most critical technology of the Industrial 4.0 revolution, has a future despite facing continuous challenges in the market. It covers impending drivers that build a stronger case for the technology. We will also discuss how the technology could benefit market players by creating opportunities for monetisation and evolving new business models. Towards the end, the report provides recommendations on the way forward.

COVID will lead to shifts towards digital supply networks

The focus of supply chain has usually been on optimising costs, reducing inventories, and driving up asset utilisation. This had resulted in strong ties to a set of limited supply chain players and consequent challenges in ability to absorb disruptions. COVID-19 illustrated that many companies were not fully aware of the vulnerability of their supply chain to global shocks.

Resilient supply chains connect with a network of suppliers. Their aim is to collaborate and optimise in real time without letting functional silos come in the way. This results in digital supply networks[i] that use technology to drive decision-making in the face of business uncertainty.

The following are some key challenges that executives need to answer in the new normal:

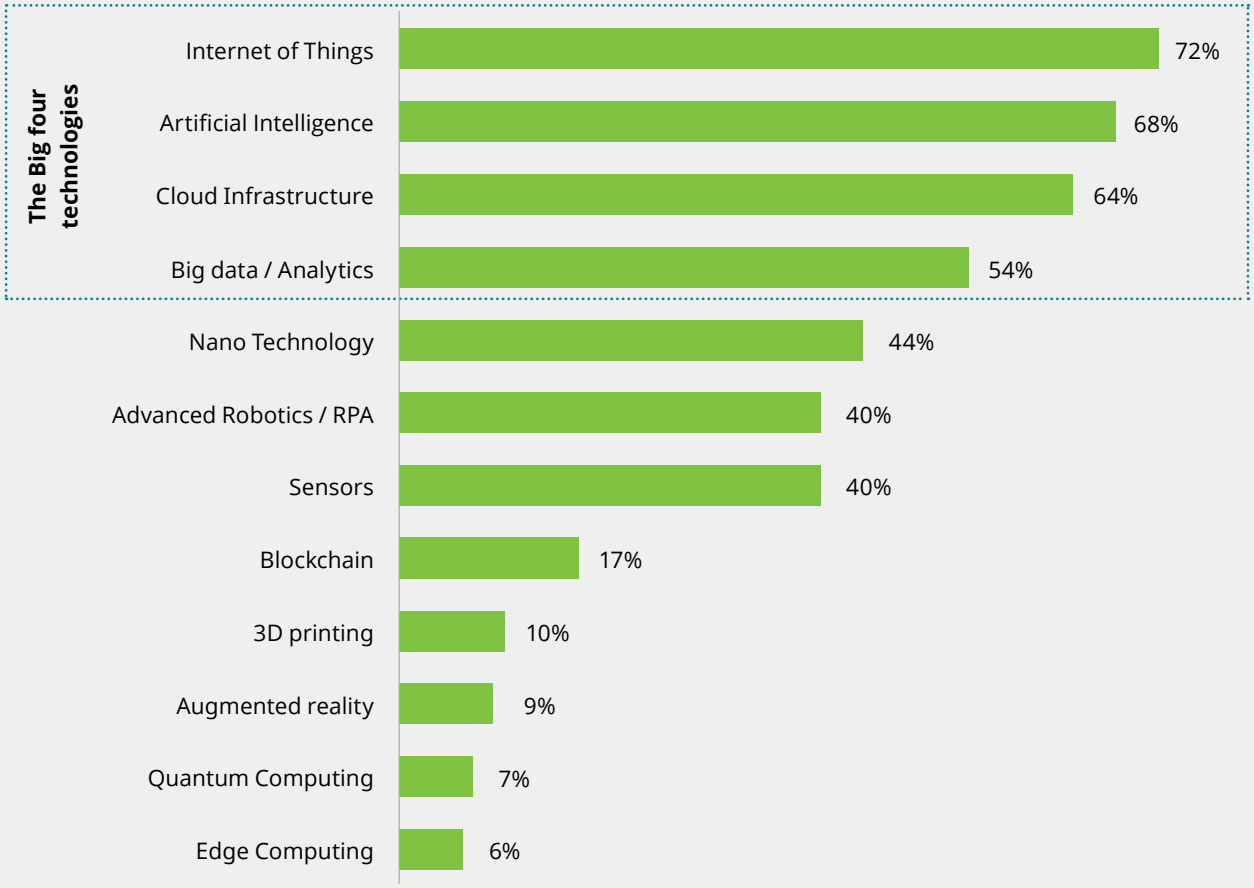
- How to balance the need to maximise asset utilisation in times of safety risks
- How to maintain safety of workers especially with respect to physical distancing
- How to deal with supply challenges due to lockdown and resulting impact on supply chains while continuing to service customers

It is also an opportunity to use virtualisation to start working digitally across locations and partner organisations.

Importance of IoT in Industry 4.0

Manufacturing modernisation relies on a set of technologies clubbed as Industry 4.0. Deloitte Global' s third annual survey[1] also took a closer look at Industry 4.0 technologies that could be CXOs' imminent priorities and have the greatest impact on their organisations.

Figure 1: Technologies by potential impact
Which Industry 4.0 technologies are expected to have the most profound impact on your organization?



N=2,029
Source: Deloitte Global analysis.

IoT, AI, cloud, and big data/analytics are the 'big four technologies' that could provide the bedrock to connect organisations, generate data, and drive more intelligent operations. Using its sensors, network, and analytics, IoT provides the core tools to automate data collection and generate insights. It is the most important component in the digital stack for the industrial sector.

In the following sections, let us understand the market potential that IoT opportunity is expected to create and the drivers that support its adoption.

The IoT opportunity

Across the world, spending on software and hardware related to IoT is projected to grow rapidly, from US$726 billion in 2019 to US$1.1 trillion in 2023, according to a market research report.[2] A recent IoT industry spending report reveals that Asia/Pacific accounted for most of the spending on IoT in 2019, with India spending US$20.6 billion[3].

After COVID-19, focus is on conserving cash in India. The following three trends are expected:

- De-growth in 2020; possibly going into H1 2021
- Companies mandated to use IoT to reimagine new ways of operating
- Growth after H2 2021 is expected to be much faster after COVID vaccine/treatment is found

The above trend is also corroborated by another recent market research[4] covering pre- and post-COVID-19 market analysis. According to this research, the industrial IoT market is expected to grow at a CAGR of 16.7 percent from 2019 to reach US$263.4 billion by 2027.

Drivers for IoT adoption in India

A few of the compelling reasons why organisations use IoT are to reduce cost and/or increase revenue, enhance safety and security, and improve product quality. Drivers that are increasing IoT adoption in the markets include the following: low cost of storing and computing data on the cloud platform; emerging trends on edge computing; falling costs of connectivity, sensors, and devices; and increasing smartphone penetration and mobile app development platforms. In this section, we will focus on key high-value drivers – cost reduction, revenue growth, security, and safety. These drivers, along with quality control measures, are expected to be critical in accelerating IoT adoption. Hence, understanding these elements and the potential use cases that could support the adoption of IoT is crucial.

Figure 2: High value drivers of IoT

Cost Reduction
Using data from IoT solutions, operators can proactively make better decisions, leading to increased efficiency and reducing operational costs.

Revenue Growth
Using data from interconnected systems, a customised offering can be created for end consumers, leading to potential revenue boost.

Security and Safety
Remote monitoring and control of critical asset supports operators in determining trends and patterns, and report any abnormality.

Quality Control
Assessing process historical data from sensors or edge devices helps operators manage the product's quality.

Cost reduction

Organisations have already started exploring more options to realise the potential of IoT by accessing untapped data and using analytics that can help operators make informed decisions in real time. With this increased efficiency, opportunities are created to reduce operational costs.

Representative case: Reducing operational costs of maintaining solar PV units and ensuring their operational efficiency at any time are becoming quite important to meet ever-increasing demand for clean energy by solar energy generating facilities within India. Using real-time data from solar PV units and custom analytical models, operators are now empowered to make real-time decisions to conduct condition-based maintenance against routine preventive maintenance that affects operational uptime of solar PV units.

Revenue growth

Data can be used to improve sales performance, reduce customer attrition, etc. This eventually leads of revenue growth opportunities.

Representative case: Retail companies can use data from disparate sources, such as CRM IT systems, store beacons, and RFID smart tags, for inventory management. This will help in better understanding consumers in terms of their historical purchase and buying patterns, and taking decisions to offer personalised services (increasing revenue growth potential). This could give an edge to organisations over competition.

Security and safety

With the help of IoT, organisations can realise their efforts to focus on ensuring a safe working environment and their employees' wellbeing.

Representative case: Manufacturing organisations have deployed security cameras and provided wearables devices to employees. These devices continuously track and monitor employees' activities. Using the data generated from these IoT devices and analytics, ensuring a safe work environment has become relatively easy for organisations.

Quality control

Processing data at each stage has helped organisations control quality and enabled operators to take corrective actions in real time (rather than checking quality after batch production).

Representative case: In thermal power generation stations, checking coal quality in real time has helped operators make necessary changes to the process of maintaining power generation efficiency.

Many sectors use IoT to achieve one or more values from these drivers. The following section demonstrates application of IoT within these sector themes.

Sector themes driving IoT growth in India

The Indian market has the following three sectors: enterprise/industrial, consumer, and services/public. Each segment has distinct characteristics and market opportunities. COVID-19 is expected to further accelerate the investment pace in IoT.

Enterprise/industrial: This segment is driven by manufacturing and product development. The life sciences, discrete manufacturing, and process manufacturing industries, along with utilities, will be spending most on IoT solutions in the coming years The trend is expected to continue with the majority of the use cases focusing around enhancing asset tracking and asset life with condition-based maintenance and equipment tracking and the ability to enforce physical distancing.

Consumer: Focus on customer experience has driven investments in this sector. Smart home and connected vehicle are expected to drive investments in IoT. The consumer sector is expected to overtake process manufacturing to become the second-largest source of IoT spending by 2023[3]

Large-format commercial retail, and travel and transport hubs (such as airports) are also likely to invest in IoT-based solutions as a direct result of COVID-19.

Services/public sector: The Government of India (GoI) has taken several initiatives (discussed later in the report) that have encouraged most of the IoT spending. Considering the government's plans of launching 100 smart cities, 500 rejuvenated cities, and numerous projects to create industrial hubs, the segment has a substantial potential for IoT spending.

With IoT software spending totalling US$39.3 billion in 2019[3] in APAC region and the fastest growth (a CAGR of 14.4 percent) expected over the five-year forecast period (2018-23), let us understand the industries that are making significant investments in IoT technology and promoting its growth in India.

Figure 3: Key sector themes driving IoT growth in India

Segment	Enterprise/Industrial	Consumer	Services/Public Sector
Representative value opportunities	• Planning and inventory • Factory and Operations • Supply network and Logistics • New business models • New products and product development • Asset Management	• Customer Experience • Channel Connectivity • Aftermarket Support • New products and extensions • Lifestyle enhancement	• Health care delivery • Commercial building energy management • Public sector safety • Public sector traffic management • Crop yield management

Major industries driving IoT investments in India

The power industry is expected to be one of the big drivers for IoT

About 90 percent[5] of India's energy comes from fossil fuels; of which, nearly two-thirds come from coal, which is a major contributor to increasing carbon emission.

Recent studies indicate that smart grid systems, which can automatically manage power flow and self-healing capability using IoT, could reduce greenhouse gas emission by about 4 percent by 2030[6]. Such smart grids (with IoT-enabled devices managing the power supply network) will have the ability to auto detect changes in power usage within their network and adjust, thus contributing to lowering carbon emission. Grid operators need to start/ are investing in IoT to make grids smarter.

Distribution companies are investing in IoT at a sub-station level to better forecast demand. In addition, use of a smart electricity meter enables real-time, two-way communication between consumer and utility. This also enables better load prediction and provides more consumer friendly services. The power ministry is driving a programme to deploy smart meters across India. Smart meters are likely to enable more IoT-related use case development.

In a renewables-heavy generation scenario, grid stability is a complex problem that benefits from IoT systems. It has enabled operators to efficiently manage quality of coal and maintain efficiencies in generating power; ensure more condition-based maintenance; reduce operational costs; support more real-time monitoring and control of processes within generating stations; etc.

Renewables are powering investment in IoT

The generation of renewables is increasing in India on the back of the public policy push and is rising much faster than that of thermal power. GoI has set an ambitious target of achieving 175 GW of renewable energy capacity, including 100 GW of solar energy and 60 GW of wind energy, by 2022[7].

Operations and maintenance of solar and wind farms are usually found to be inefficient given the geographical spread of plants. Operators need to cover large distances to identify the nature of faults in plants. Using IoT and analytics-based centralised monitoring and fault case diagnosis, generation operators are seeing significant business value in IoT.

The rise of renewable plants poses unique challenges to India's coal-based base load plants. In the absence of gas-based flex capacity in power generation, coal-based plants in India need to operable under variable load conditions. To manage such variable demand, power generators are investing in IoT to better sense and plan for plant loads.

IoT solutions transforming the healthcare sector

Smart watches, fitness bands, monitoring patches, and heart rhythm detectors are examples of IoT-enabled devices that already exist to capture and monitor healthcare data. After COVID-19, the healthcare sector will renew its focus on technology enablement to cope with higher expected load on care facilities.

Potential applications of IoT that are likely to emerge in the healthcare sector in India are mentioned below:

- Real-time access to patient data and improving workflows via sensor-based smart chips, real-time location systems, etc.
- Use of connected thermometers for workplace health monitoring
- Use of connected devices for remote patient care
- Supply chain traceability for pharma

Smart agriculture can create an exponential impact

The far reaching impact of climate change on agricultural production is likely to challenge food security in the future. The agricultural sector has realised the need for investing in a technology that enables monitoring soil, weather, and crop conditions.

Government of India is advocating the use of sensors in agriculture value chain.[ii] The deployment of IoT sensors to collect and transmit data in agricultural activities will lead to the development of advanced techniques in precision agriculture monitoring. This means avoiding years of wasteful over-consumption of water, fuel, and soil additives, as well as limiting the use of pesticides and fertilisers. IoT devices could also increase the reliability of weather forecasting processes, thus enabling farmers to make more efficient use of their resources and reduce waste.

Pharmaceuticals focussing on supply chain visibility

Pharmaceuticals is one sector that has seen its outlook improve after COVID 19. Categories such as therapeutic and over-the counter medicines saw supply-side disruptions and demand contraction. Manufacturers are looking for AI-based demand sensing algorithms to simulate multiple scenarios and plan their distribution well in advance.

Companies focussing on supply chain visibility and demand sensing as the two main use cases for IoT-enabled projects find Industrial Internet of Things (IIoT) is the best way of getting quality real-time data across the enterprise. This in turns allows for AI models to become more accurate and provide an opportunity for pharma companies to gain visibility to the nth tier in the complex pharma value chain.

Specialty chemicals are focussing on supply chain diversification

Specialty chemicals is another sector that has benefitted from COVID 19 disruptions. Traditionally, China has been the top supplier of specialty chemicals across the globe. However as supply chains diversify out of China, Indian specialty chemicals manufacturers ramped up to increase their volume share. This ensured that demand has gone up significantly in the export market for India-based specialty chemicals companies.

Companies in this sector are primarily looking at solutions to connect with the global supply chain through planning integration and demand sensing. This is a growth sector

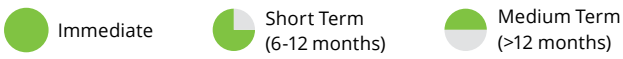
in India. In the post-COVID-19 world, the focus of specialty chemicals companies has been on tapping greater growth and integration with global supply chains.

Other sectors, such as automotive, metals, and mining, are also deriving significant value from IoT. Therefore, this allows us to predict that IoT is expected to become a key investment area around later 2021 once cash flows improve.

Figure 2: Relative relevance of advanced technology use cases across industries in a post-COVID-19 scenario.

Segment	FMCG	Pharma	Cement and metals	Specialty chemicals
Command centre				
Demand sensing and scenario planning				
Direct to customer (e-commerce and marketplace aggregators)				
Quality sensing and detecting				
Predictive maintenance				
Advanced worker solutions				
Plant consumption and energy management				
Supply chain "Digital Twin"				
Smart conveyance				
Smart work-in process warehousing solutions				
Augmented efficiency and safety solutions				

Source: Deloitte Internal research



IoT technology creates opportunities with exciting new applications for many industries. However, it also brings unprecedented challenges that require thinking in new ways to meet mission-critical requirements. Let us understand some of the key challenges and select aspects that companies should plan for IoT investments to derive better business benefits.

What has held back IoT adoption in India

The transformational nature of IoT has not been a matter of debate. However, at least in India, adoption of IoT has still been somewhat at the niche stage. Some of the key challenges that need to be addressed are mentioned below.

Lack of clarity on what to prioritise

Behavioural studies[9] suggest that people are more likely to invest for the future if they are presented with fewer, not more, investment options. As capital investment is being fought over by multiple use cases, adopters of IoT are organisations that have typically followed a KPI-driven digital strategy to identify and track key IoT use cases.

Lack of vision and short-term value realisation

Most sectors in India are not at a big scale. Hence, typical IoT conversations are transactional in nature and typically funded by individual departments. This has led to challenges in adopting the right platform that could lower the overall cost. Therefore, the overall return on investment has not been exciting for management. This also implies that interventions in connected operations have been incremental and not transformational in nature.

Organisations should consider investing in technologies such as IoT during the downturn and be ready to operate.

Research[8] suggests that companies that invest in key technological advances during downturns such as the one we are facing due to pandemic are better positioned to leapfrog competitors when economic conditions improve. Therefore, executives should consider using the current time to plan and execute their IoT agenda.

Lack of right talent and skills for implementing and maintaining IoT ecosystem

Talent and training continue to be focus areas for leaders, and consistently rate as a top concern and challenge with respect to navigating digital transformation. In a recent study, 74 percent[8] leaders noted that they prioritise core technologies within Industry 4.0 investments for "training and developing a workforce with the skills needed to compete". With that in mind, talent development appears to be an area of ongoing focus that requires concerted efforts, adaptation to ongoing changes, and a disruptive mindset to drive transformative efforts across the organisation.

We see a focus on developing talent. GoI policy making organisations, are talking about IoT and working to develop the ecosystem in India.

Technical challenges of connectivity, compatibility, interoperability, and cybersecurity

IoT needs a healthy ecosystem of vendors, OEMs, and service providers. Connections between devices and systems are a recurring challenge for implementers. Interoperability between systems is one of the major reasons contributing to failure of IoT implementation.

Traditional cybersecurity protection solutions have focused securing IoT network and cloud infrastructure. Endpoint and over the air (OTA) vulnerabilities are frequently overlooked. Endpoint devices need to be thoroughly tested and kept updated for threat/attack definitions.

Due to the COVID-19 outbreak and the subsequent supply chain disruptions, the same set of challenges have re-surfaced with a greater emphasis on business case and ROI justification. A new set of challenges have been added to this list in a post-COVID-19 scenario.

- Very short (current quarter) timeframe to evaluate solution performance
- Identifying the remote capability for solution deployment and minimising human involvement

With its large bandwidth and low latency, 5G network is uniquely suited for IoT connectivity. Investment in 5G in India has been lagging for various reasons. However, recent announcements by leading vendors on starting 5G trials in India are likely to lead to cheap and ubiquitous network connectivity after the network rolls out.

Obtaining an in-depth understanding of challenges with robust design throughout IoT implementation lifecycle will help ensure that IoT delivers on its promises. This will also help build a strong foundation for using IoT across the ecosystem. In the following section, let us understand different stakeholders/market players in the ecosystem and how IoT technology is changing their roles and ways of operation.

Developing the IoT ecosystem

Technology adoption requires a healthy ecosystem of buyers, consulting advisors, hardware suppliers, technology implementers, and talent organisations. Market players are changing in their own ways to support the growth of IoT deployment across sectors. Let us look at how the four key players − technology consumers, technology providers, R&D institutions, and policymakers − are seen supporting this technology.

Buy-side ecosystem changes

Shifting from being just a consumer to a prosumer: Buyers are focusing more on using data and insights gathered from multiple devices. They have started exploring opportunities to monetise this data and create new business models. This is seen changing the way buyers look at technology.

The dividing line between consumers and providers is diminishing as large consumers are trying to create their own offerings: While designing the digital transformation journey, consumers have started focusing on the aspect of incubating innovation internal to organisations by collaborating with start-ups, partners, suppliers, and research institutes. With this changed operating model, consumers have become open to partnerships to either build solutions with the help of an ecosystem of firms or are looking to buy innovative solutions and stitch these solutions together to create more mature offerings. This is likely to diminish the line between consumers and providers of technology in the market.

Traditional technology providers are evolving and diversifying their focus from only implementing solutions towards enhancing value creation

Building standards and interoperable systems: At present, many proprietary systems exist that are not easy to connect to other platforms. This makes developing large-scale systems difficult. Technology providers have the capability to develop and provide solutions that are built on open standards and interoperable with other proprietary systems. Such capability could allow business firms to tap into the innovation ecosystem described above, and use innovations from start-ups and other players by quickly plugging innovative products into their business platforms.

Shift towards service model: Technology providers are moving away from the traditional model of providing a product solution and charging on usage licence, towards a service model with pay per use capability enabled for consumers.

Brownfield innovation: Technology providers produce industrial products that are built to last longer. They have started building solutions to support their existing products deployed at consumers' premises that otherwise had a defined obsolescence lifecycle. By working on identifying what sensors or devices can be added without compromising systems' integrity, technology providers are identifying new value-add services to make such equipment more productive, intelligent, and efficient.

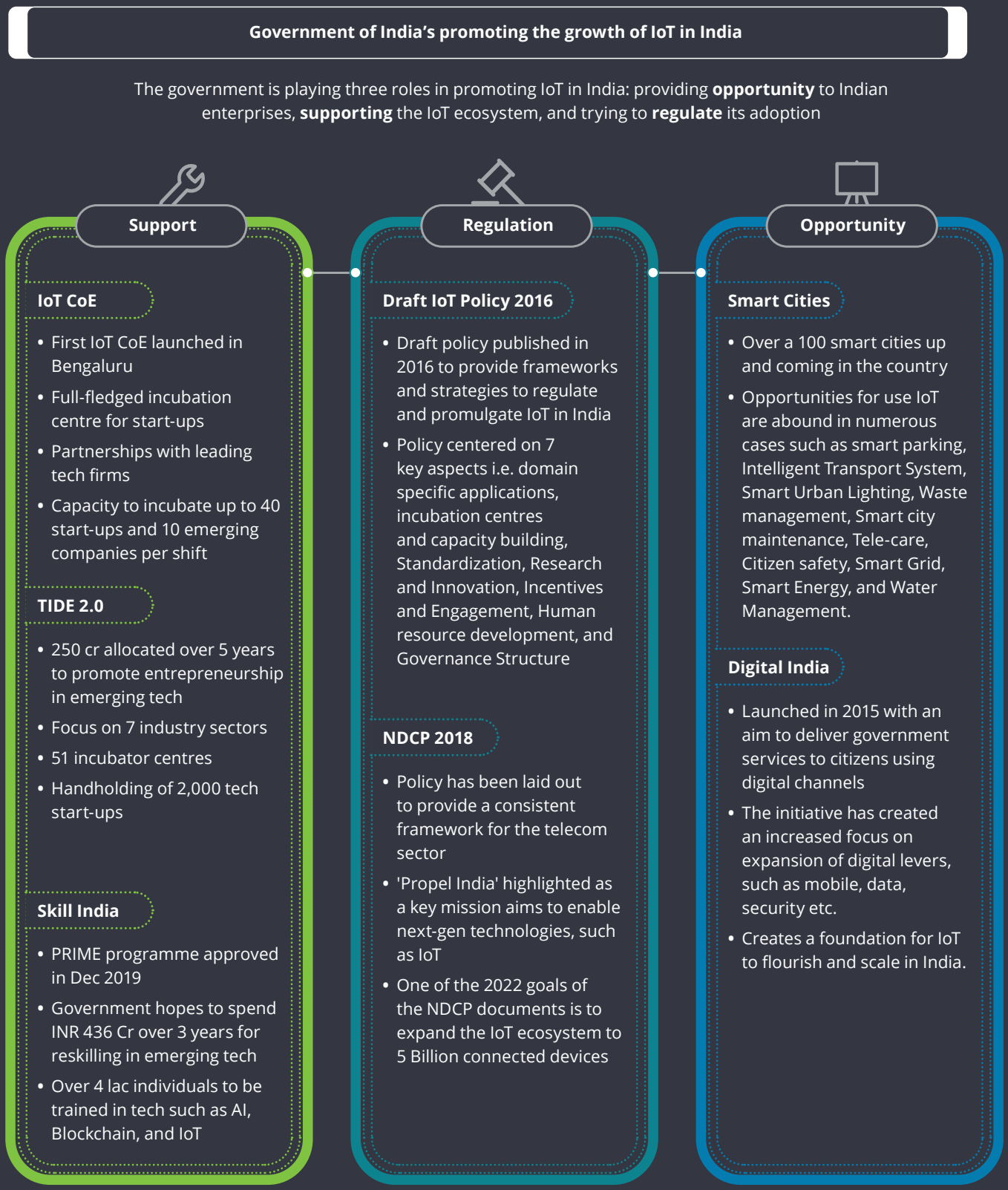
Academic institutions are enabling innovation and solving industry problems using IoT

Environment for research and development: Academic institutions have started playing a critical role in today's world. These institutions can support consumers and providers to provide real-world test-environments to demonstrate how proprietary solutions from different OEMs can work together to support new use cases and product concepts at scale. Participation from technology providers and consumers in such ecosystems gives these stakeholders a direct voice in shaping future industrial products and services using the IoT technology. It is could also provide an early-mover advantage as they gain a better understanding of requirements, trends, and possible timing around potential market disruptions.

The impetus from policymakers to encourage IoT adoption in India is crucial

Given the relatively high cost of capital and lower capacity to invest in the Indian private sector, public push via policy and incentives could go a long way in modernising core sectors via IoT. GoI has taken various initiatives to promote the technology's growth in India. Some key initiatives in three areas are mentioned below.

Figure 4: Role of Government of India in promoting IoT adoption

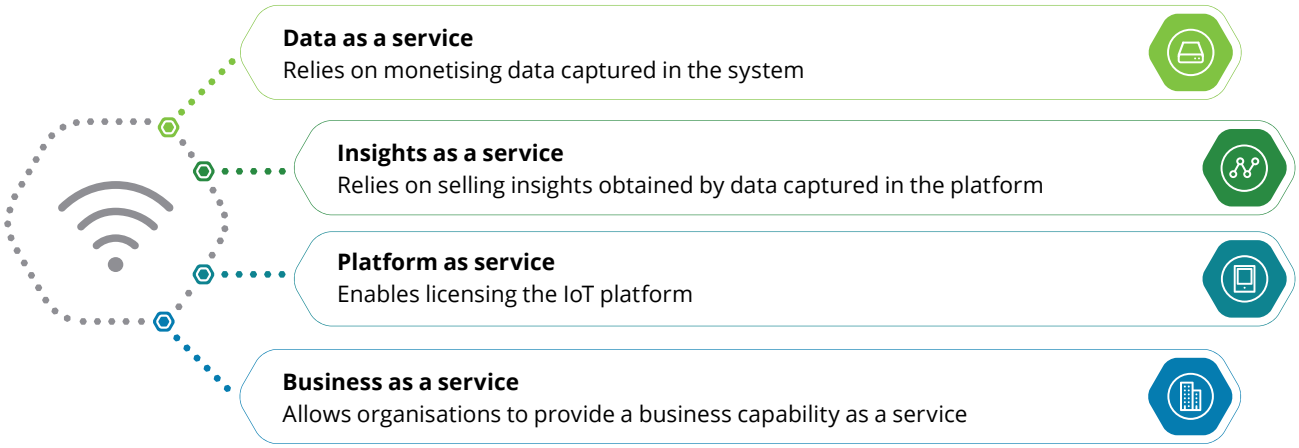


These programmes are expected to help drive the adoption of IoT technologies. Given the geographical spread of India and variations in economic maturity, more of these state-driven interventions focusing on modernising the key sectors for those states could go a long way in realising the full potential of IoT technologies. The expected growth of IoT will help create new market opportunities for monetising outcomes of IoT projects. The combination of data and algorithms matured within the firm could allow most organisations to offer these business platforms to other similar players in a variety of models.

With this understanding of the roles of different stakeholders in the IoT world, let us explore the evolving new business models that create an opportunity for IoT monetisation for these stakeholders.

Revenue opportunities driven by IoT

When IoT shifts from being a cost to a revenue generator, companies realise the maximum benefits of connected operations.. Monetisation opportunities typically are driven by various data monetisation models, including the following:



Let us look at each of these models in detail.

Data as a service: In this business model, organisations can collate and aggregate the data being generated by IoT devices and sell it to end-consumers or data aggregators in the market. End-consumers can build their own custom models or algorithms to generate insights from this data. For example, telecommunications companies provide aggregated and anonymised customer geolocation data to local governments, allowing city planners to design better traffic management systems and officials to better establish "smart city" technology solutions.

The emerging trend of home automation is another example for the "data as a service" business model. For example, many IoT devices collect end-consumers' data from home automation. This could help consumer goods manufacturing organisations tailor their product features or target a specific customer segment to increase their revenue.

Insights as a service: In this business model, organisations may combine internal data (for example, sales and operations trends, and machine performance pattern) with external data (such as company data from third-party platforms or other open-source platforms). Thereafter, these organisations may apply advanced analytics algorithms/models to derive insights to be sold to end-consumers. Insights as a service is a software service that provides actionable information and a plan to use that. The service is delivered just like any other software as a service product. It is hosted on the cloud and end-consumers may subscribe to such services.

Typical examples is SaaS IoT platforms conducting predictive analytics on day 1 using historical performance of a machine's make and model that they already support. Some specialised SaaS IoT start-ups are taking this route.

Platform as a service: Organisations build custom and proprietary algorithms to generate enriched, customised real-time data delivered to customers via cloud-based, self-service platforms. With the support of in-built custom models, this business model mainly provides a series of analytics features. These features enable business analysts to diagnose and discover key patterns and insights in their data and applications. Such a model also provides a set of visualisation and dashboard capabilities that can enable operators and executives to make rapid business decisions and maximise business value.

Traditional IoT software vendors have followed this route.

"Business as a service" is expected to be logical evolution

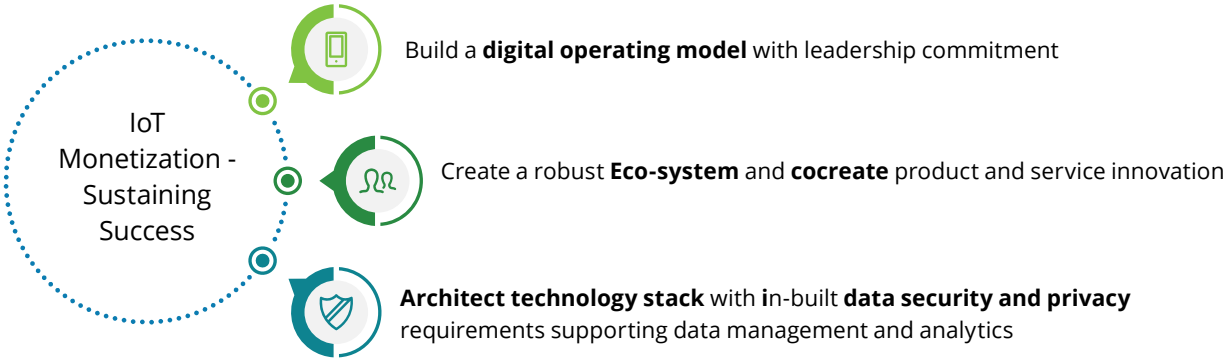
Organisations usually invest heavily in capital assets, and spend a huge amount on repair and maintenance activities. With the adoption of IoT, these organisations have realised the benefits of reducing such asset maintenance costs. They are also evaluating/have started exploring opportunities of creating a package formed using insights from internal IoT project exercise. These company have started providing such packaged service in the form of business as a service to other market players facing similar challenge of reducing operational costs. For example, in case of asset maintenance, organisations have started building the ability to provide maintenance-related service to other players in the market. This is being termed as "business as a service". This is becoming popular in large organisations with multiple business groups that already have separate operations and maintenance groups. These groups can typically spread the cost of building a platform across multiple units. These groups use productivity gains to profitably bid for providing operations and maintenance services based on the IoT platform to other firms.

For large organisations with multiple businesses, with a ready catchment of subsidiary firms, it could be easy to test out the business model. On the flip side, organisations will need to cultivate a product development mindset while developing their initial platforms. Such platforms can act as a disrupter for many technology firms focused mainly on IoT as business, and lead them to move from customise and configure, to primarily configure only.

Along with change in mind-set and adopting right monetization model, it is critical to adopt new ways of working for leveraging IoT technology as a revenue generator. Many savvy business and technology executives are already working together to reimagine how IoT technology delivers business value and competitive advantage. To keep pace with this evolution, let us understand key requirements enabling monetising of IoT investments, in the following section.

Creating and sustaining success

As technology reshapes traditional business practices and paradigms, organisations can remain competitive by being agile, collaborative, and customer-centric. The traditional operating model works well when the CIO's mandate is to provide back-end tools and infrastructure. Today, the technology leaders' mandate extends across the enterprise. The role of technology has evolved from automating the business to actually being the business. Organisations can follow the pointers given below to extract return on investment from their IoT projects.



Building digital operating model with leadership commitment will act as a critical enabler for IoT monetisation

In traditional business models, business functions/ departments mostly work independently. IT organisations also often had top-down organisation structures, with technology functions rolling up under a single leader, such as CIO or CTO. Such traditional operating model constructs typically stood in the way of innovation, agility, and collaboration. Only if there is a specific need, there will be cooperation with focussed objectives. As IoT initiatives are carried out and with the company's intent to monetise data, it has changed business models. Business and IT teams can no longer operate in their own isolated islands, especially if companies intend on operating in the fierce global marketplace.

No one-size-fits-all organisational structure exists for driving an IoT monetisation strategy. Although a decentralised or centralised organisational model for data-and-analytics activities can work, we suggest that a hybrid model incorporating the elements of both could be better suited to organisations. To deliver on the promise of IoT initiatives, the operating model should be agile and enable collaboration.

Departments right from IT and engineering managing data and systems through finance, marketing and operations need to work cohesively to offer product/services that help monetise on IoT initiatives.

We propose business leaders should consider five key elements for reimagining the operating model.

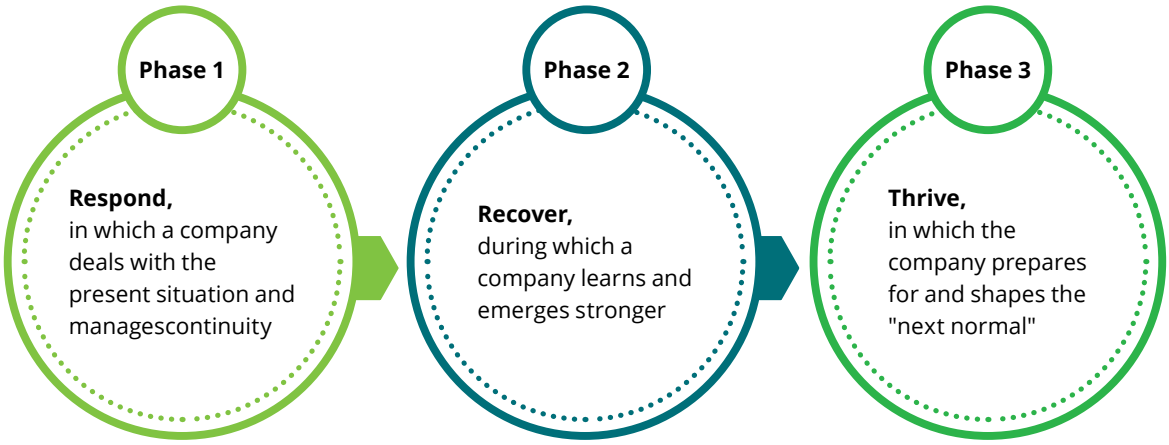
- **Business and technology strategy:** Aligning the technology function's ambition and value creation with a business-technology strategy
- **Technology ambition:** Technology driven or enabled business opportunities and markets
- **Technology capabilities:** Build tech capabilities required to achieve business-technology ambitions
- **Modes of operation:** Align tech organisation, i.e., change from traditional support mode to revenue generator, and a model for implementing the technology

- **Organisational transformation:** Transform across multiple dimensions, i.e., redesigning organisation structure, embracing a broad workforce ecosystem, and rethinking culture

Designing an agile operating model is critical in the long run for deriving value from IoT investments. At the same time, understanding the prevailing market forces driving business operations is essential. With COVID-19 causing economic damage, business leaders are concerned about how their companies will be affected and what they have to do next. We are proposing a resilient leadership framework with elements as Respond, Recover, and eventually, Thrive for companies, to act during the pandemic.

Need for resilient leadership in the face of COVID-19[10]
Companies should think ahead to be in a state of readiness to resolve the challenges due to pandemic and protect the future of the business. As a business, we recognise that there is no "one size fits all" solution to tackle this situation. Regardless of the extent of the virus's impact on an organisation, we believe that a typical crisis plays out over the following three phases:

Figure 6: Resilient leadership Framework



Within the framework of these broad imperatives, resilient leaders can take specific steps to elevate these qualities during the current crisis, blunting its impact, and helping their organisations emerge stronger. With the right approach, this crisis can become an opportunity to move forward, create more value, and make a positive impact on society.

Building a robust ecosystem of partners, suppliers, and service vendors to support and co-create IoT products and monetisation services

Companies are expecting quicker and easier integration of IoT solutions with their enterprise systems and applications to realise a faster return on their investments. More companies are seen expecting value through integrated solutions. However, developing and delivering these integrated solutions is often challenging for a single company to address independently, cost-efficiently, and effectively. While companies should continue to invest in robust internal R&D capabilities, today's changing business environment indicates that companies expand their sources of innovation.

A model of cooperative innovation—an ecosystem—is increasingly becoming critical to drive value for the parties involved. We see this as co-creation—strategic partners actively collaborating to create and deliver customer-centric products and services (offers) that capture greater value, more rapidly and at a lower risk than traditional product-development approaches.

An ecosystem of partners, suppliers, and service providers is important to derive the maximum potential of monetisation. Organisations should focus on creating a marketplace where partners can host information on cloud, enabling easy access to information anytime and anywhere. Opening up this to third parties is beneficial, and makes it easy to build and publish apps, and custom solutions to generate revenue.

One key component of the ecosystem is academic and research institutes. These institutes are key drivers of innovation. For example, some universities support smart city solutions.[iii] Apart from being skill providers, academic institutes can support long-term research[iv] in a particular area.

Strengthening core foundations – Technology stack with in-built data security and privacy

Building a robust data management and analytics strategy is imperative for organisations to derive maximum insights from data. Organisations should design their technology stacks that support collecting data in structured and unstructured formats and have an intuitive interface that enables analysis, synthesis, modelling, and interaction with data. The goal is to create a "single source of truth" via data storage, harmonisation, and processing.

To make such a data platform effective, the focus should be on building an interoperable system that creates an internal ecosystem for the seamless exchange of data and information from varied sensors or devices (compatible with different OEMs and their proprietary communication protocols). The focus should also be on using open communication standards across technology systems that enable ease of information exchange.

Rapidly increasing use of IoT devices and connectivity within organisations create potential vulnerabilities. This makes it imperative to design and incorporate data security and privacy requirements since the start of any IoT implementation project. With increasing cyber risks and attacks, we have given a special focus on how companies can be better prepared to manage data security and privacy challenges in the following section.

Addressing data security and privacy challenges

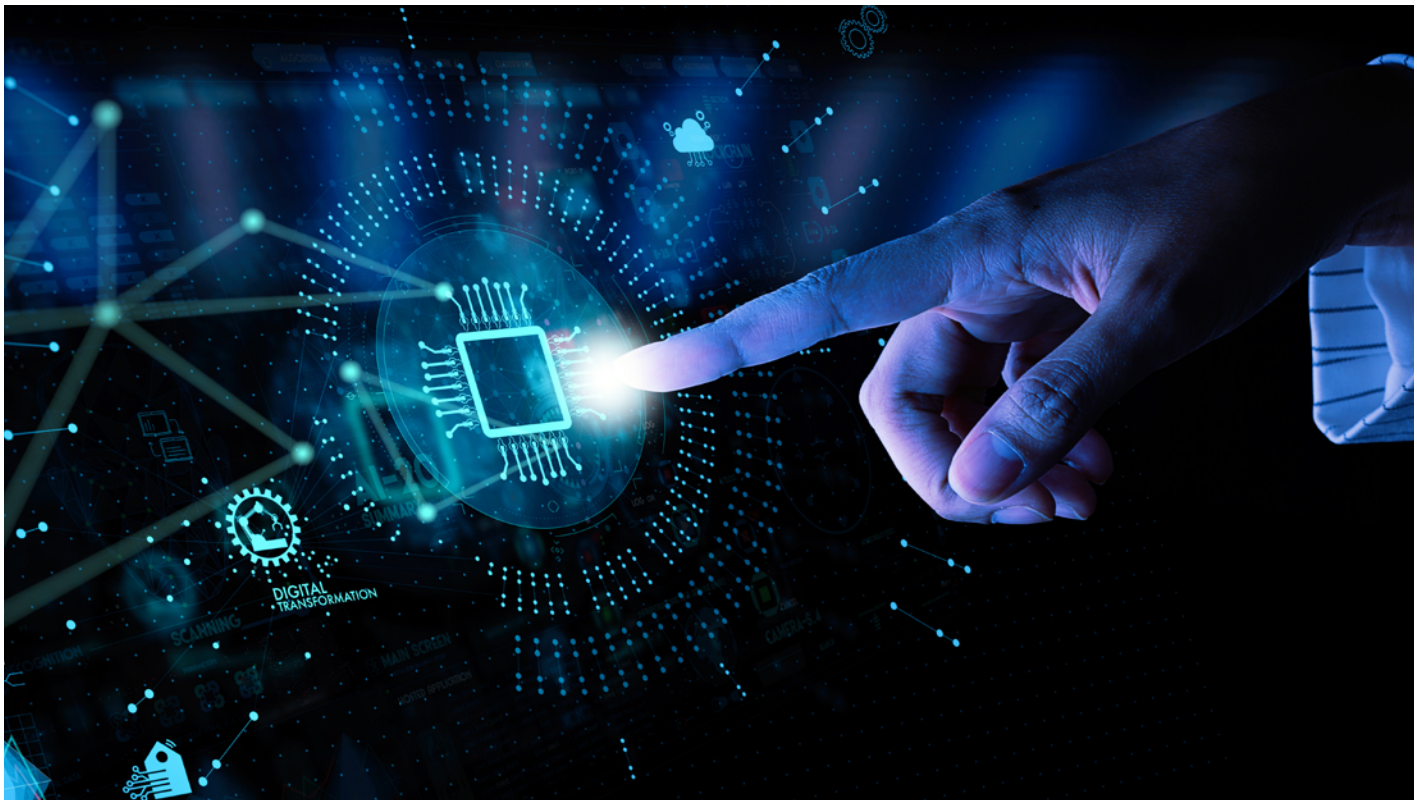
The rise of connected world is also expected to bring challenges around ensuring that sensors and edge devices do not become a threat vector or get hijacked; the captured information is used and storeda securely; and privacy rights are respected while collecting and using data.

Data protection and privacy plays a key role in the IoT landscape, which holds a close relationship with cyber physical systems (CPS) per NIST SP 1900-202. The IoT platform helped in interweaving various technology platforms and operational environments. It ensures flexibility and extended use of the generated information across industry business verticals to carry out refined data analytics (supporting better decision-making and anticipating future events). IoT is continuously driving innovation in business models through digital transformation, which is more than just interconnected objects, across industry verticals.

However, with the rapid emergence and expansion of diverse technology platforms, data security and privacy are major concerns in the overall interconnected business operational model, specifically around the following:

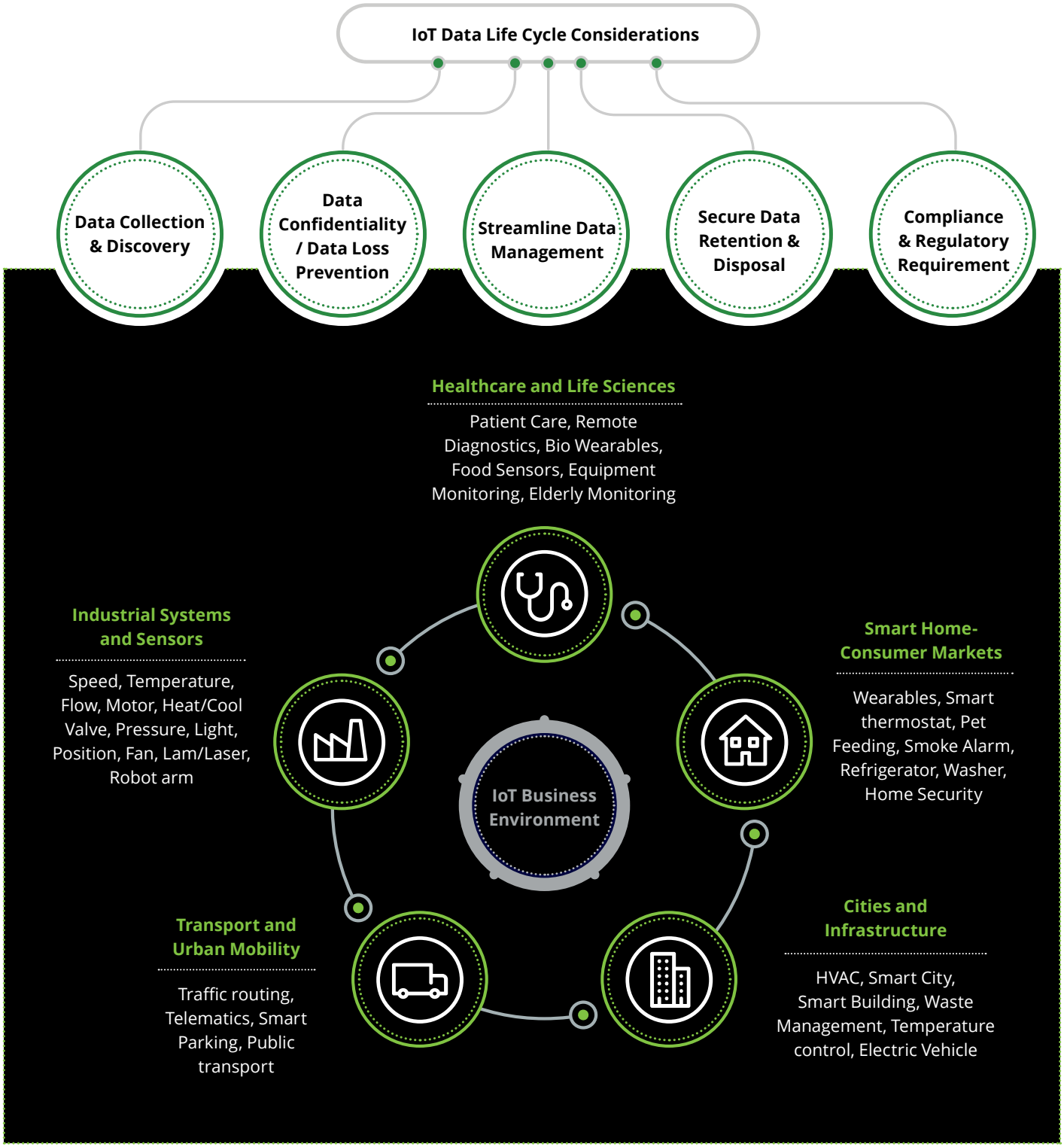
- Blurred perimeter boundary
- Dynamic nature due to continuous mobility
- Platform physical security challenges
- Involvement of and dependency on interested external parties

According to the root-cause analysis, for the common identified vulnerabilities associated with the IoT platform, the Open Web Application Security Project (OWASP) majorly indicates the immature enterprise cyber risk security framework and absence of integrated risk management approach for end-to-end data life cycle management.



Securing the data life cycle in IoT

Figure 7: Integrating End-End data lifecycle with IoT verticals



- **Data collection and discovery:** As the adoption of IoT gains pace, collecting and then analysing vast quantities of data produced by billions of devices within the IoT ecosystem is vital. IoT data collection and analysis are now critical skills to have within an enterprise.
- **Data confidentiality/loss prevention:** The critical information collected through the interconnected IoT platform should be encrypted at the transport layer and at the rest state using strong encryption, data integrity checksums, and data loss prevention mechanism. This will help ensure the confidentiality and completeness of the sensitive data.
- **Secure data retention and disposal:** Ensuring secure data retention and disposal, coupled with data minimisation, is a huge regulatory imposition for carriage service providers and internet service providers (ISPs) in the ever-growing IoT device ecosystem. The regulation also acts as a disincentive for any third party intending to partake in any services that combine carriage with data management.
- **Compliance and regulatory requirements:** Due to the dynamic nature of how IoT systems deal with personal identifiable information (PII), regulatory authorities must ensure that PII is processed in ways compliant with regulatory and organisational policies.

Key security and privacy challenges

Security challenges

The IoT platform can intertwine nimbly across business-sector platforms, raising security concerns pertaining to the collected information and effective management. The following are some observations per industry analysis:

- **Weak authentication/authorisations:** Researchers notify that a vast majority of the people use IoT devices with weak passwords, and insufficient authentication and authorisation.
- **Lack of comprehensive management**: IoT service providers have to cover a lot of ground in terms of maturity in IoT device's data and device lifecycle management, and provide administrative coverage. This is because IoT owners might not entirely manage an IoT device's firmware, operating system, and applications. They may not have control over aspects such as data retention and subsequent sanitisation of personal data from the backed data repositories.
- **Lack of notification:** Some IoT devices lack application and/or human user interfaces for device management, leading to inability to acquaint concerned individuals to provide meaningful consent for processing their PII. This situation is worsened due to lack of universally accepted standards for IoT APIs, thus fostering interoperability among IoT devices.
- **Limited encryption capability:** Encryption protocols and a centralised key management solution need to be engineered to be efficient, scalable, and compatible for deployment on large-scale IoT systems and devices with limited computational resources. The system should also address the increased complexity of data movement through the integrated IoT world.
- **Insecure web interface:** A vast majority of IoT-based solutions have a web/mobile interface to consume collected data and send it across service providers. The web interface is found to be more prone to the OWASP top 10 vulnerabilities, such as poor session management, weak default credentials, and cross-site scripting vulnerabilities.
- **Periodic security upgrades and increased threat vector:** Considering the volume and nature of integration in the IoT world, regularly upgrading security patches will be a tedious and complex job.
- **Use of default IoT parameters:** About 70 percent of the devices and sensors are configured to use the vulnerable factory-set default usernames/passwords.
- **Diverse nature of collected data:** Decentralised data processing functions and assorted ownership of IoT devices challenge traditional accountability processes. This may result in individuals not being able to locate the source of inaccurate or otherwise problematic PII to fix the problem.
- **Data portability and interoperability issues with vendor lock-in:** Due to interoperability challenges, consumers face the risk of getting locked-in with a specific IoT service provider that may hinder data portability flexibility for end-customers.
- **Continuous availability:** IoT platforms' ability to unceasingly defend against relentless and persistent attacks, such as denial of service (DOS) attacks, is precarious as an entire underlying ecosystem of dependent systems may be affected. The key challenge is to ensure the availability and continuity in the provision of IOT services, and avoid any potential operational failures and interruptions.

Privacy challenges

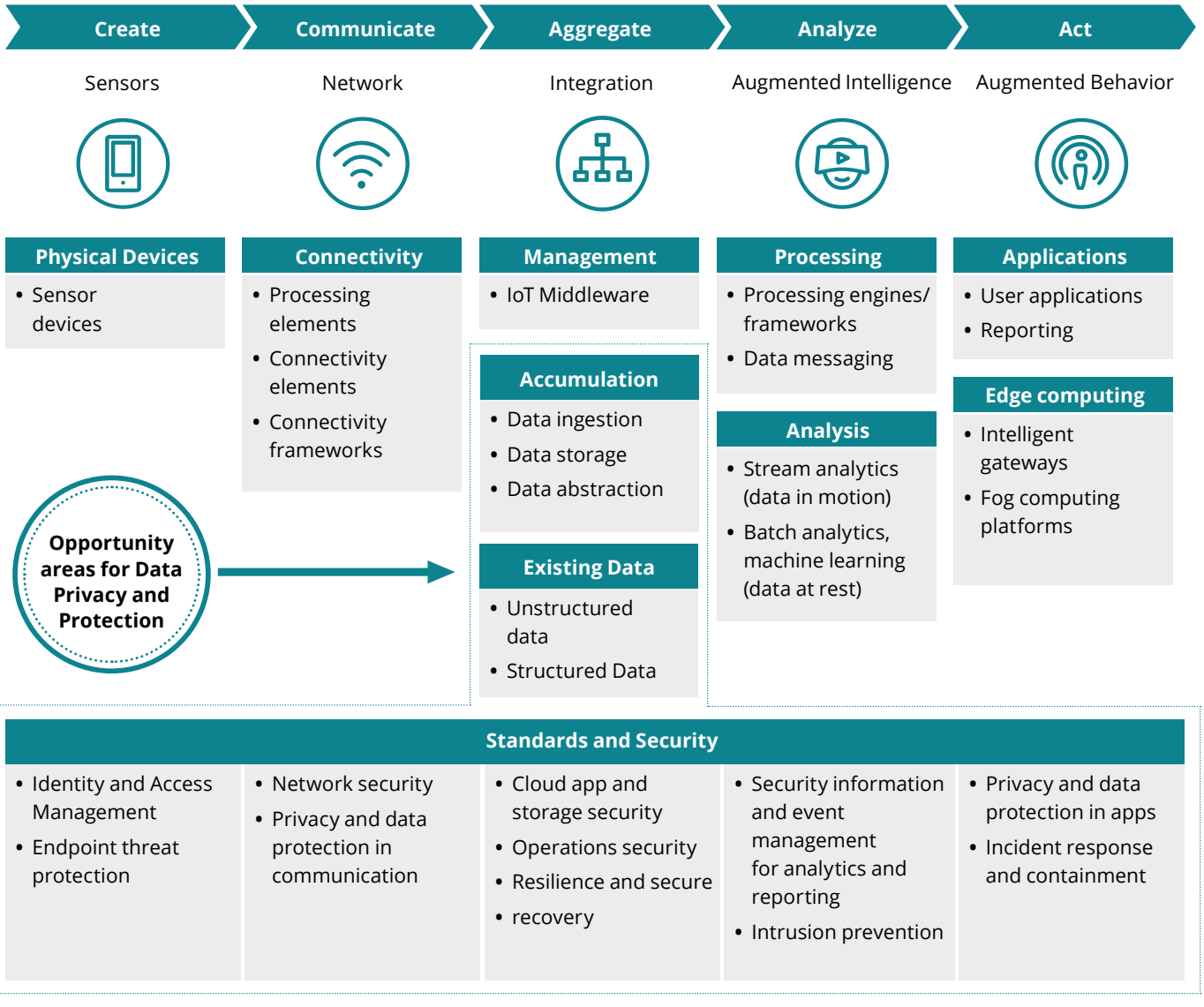
IoT systems collect information that may be a personal or business secret. Implementations need to ensure better management of the following:

- **Privacy by design:** Due to dissimilar nature of elements functioning together in IoT, the identification and treatment of privacy risk becomes a challenge. IoT elements, such as sensors, objects, and applications, come with their own sets of risks and controls.
- **Data subject rights:** Due to the blurred perimeter boundaries, IoT uses data collected from different sources and objects to identify individuals. In such scenarios, ownership and exercise of data subjects' rights become a challenge for both data controller and data processor.
- **Emerging privacy regulatory and compliance requirements:** This challenge is exponentially amplified as collection, processing, interpretation, and application of the resulting data could take place in different jurisdictions with varied rules and regulations (due to the global nature of IoT devices and use of different networks/sensors/objects/applications).

Key considerations for privacy and protection in IoT

IoT cyber security framework with inherent privacy and protection

Figure 8: Integrating Data Privacy & Protection with IoT Cyber Risk Security Framework



To counter the increasing threats in the IoT landscape, IoT's core development and architecture design should follow a secure-by-design approach.

01. **Security and privacy by design:** Due to the ongoing disruptions caused by IoT in the consumer, enterprises, and government sectors, adhering to security and privacy by design principles should be imperative to enhance consumer privacy and security, and build consumers' trust in IoT devices. This holistic approach enables the IoT landscape across business industry platforms to weave privacy into the very fabric of IT systems, networked infrastructure, business processes, and design specifications.
02. **Unified security guidelines:** The decentralised and distributed nature of IoT systems makes it crucial to have unified and well-designed security guidelines (enabling encryption in transit and at rest), and trust establishment across the connected devices with a secure centralised certificate and key management.
03. **Compliance check for third parties:** The involvement of third-party services may introduce new security breaches, making it vital to evaluate compliance and security health checks of the involved services components.

Privacy and data transparency

Processing large volumes of personal data may result in severe privacy implications, which can be countered with the help of the following measures:

- **Data governance and privacy:** Setting up a governance framework, which at minimum adheres to applicable privacy laws, is one of the key challenges that multinational companies face.
- **Exponential increase in data volume:** Data protection needs to be considered for the data generated by IoT devices at rest and in transit; the aggregated or distributed data; and both types of data within traditional organisational boundaries and on dispersed devices.
- **Information life cycle management:** Consistent protection and management of information (starting from data creation to final disposition) needs to be ensured.
- **More nuanced privacy consideration:** IoT can create conflicts for organisations about which data is public and which is private, warranting a proactive deliberation on the subject of privacy.
- **IoT and trust:** IoT providers can win the trust of users (either individual consumers or enterprises) by ensuring transparency about what data is being collected and how it is being shared. They can also enable users to see, analyse, and act on data in real time.
- **IoT and data collection:** Companies need to outline what information is needed to deliver value to customers, and then allow users to select and only share that data.
- **IoT and access to data:** To ensure better privacy, IoT providers can allow users to control their own data by defining how and when different apps can get access to information.

Way forward

IoT as a technology has been maturing for some time and seems poised for continued growth in India.

This growth is expected to be driven by specific sectors, such as agriculture, utilities, manufacturing, and infrastructure that are responding to big changes in their operating environment. IoT is also being adopted in the consumer goods industry to enhance user experience. Government policies and interventions can help further accelerate IoT adoption.

Expected significant cost savings and new revenue lines based on business IoT platforms are likely to make IoT adoption a priority for CEOs. The firms investing in IoT will need to adopt newer ways of working and operating models to implement the technology in a way that can sustain IoT projects and support changes in ways of working with new business models.

To further accelerate the adoption, industry, technology providers, and policymakers (government) need to work together to address the challenges discussed in this paper.

Technology providers should focus on designing and developing India-specific products and solutions that are price competitive within the Indian context. The stakeholders in the IoT world should build a collaborative ecosystem that supports buyers in starting their transformation journey, by providing best practices, feasible use cases, and operational models. COVID has presented an opportunity for technology players, including small and medium enterprises/companies (SME) to build an IoT ecosystem, and adopt virtual ways of working and maintaining social distancing.

The industry and academia should tie up to research on India-specific localisation requirements for IoT systems to work seamlessly in Indian conditions. This tie-up will also help create a talent pool that will allow the percolation of the IoT system down the enterprise value chain.

Such transformative technologies do not come without challenges. Pervasive issues need to be addressed in a rapid and thoughtful manner. These issues include security and data privacy; availability of a cheap network over a wide area; interoperability among platforms; and availability of skills especially around machine learning and artificial intelligence. While plans and policies are a great start, relentless execution is also needed to drive IoT adoption. With the focus on Digital India, National Skills Development Mission of India, and STEM (Science, technology, engineering, and mathematics) education, GoI is driving India to overcome many of these challenges.

IoT technologies offer tremendous growth opportunities and India has set the stage for becoming an IoT powerhouse.

About Deloitte

All the facts and figures that talk to our size and diversity and years of experiences, as notable and important as they may be, are secondary to the truest measure of Deloitte: the impact we make in the world. So, when people ask, “what’s different about Deloitte?” the answer resides in the many specific examples of where we have helped Deloitte member firm clients, our people, and sections of society to achieve remarkable goals, solve complex problems or make meaningful progress. Deeper still, it’s in the beliefs, behaviours and fundamental sense of purpose that underpin all that we do. Deloitte globally has grown in scale and diversity—more than 312,000 people in 150 countries, providing multidisciplinary services yet our shared culture remains the same.

About Confederation of India Industry

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

For 125 years, CII has been working on shaping India's development journey. This year, more than ever before, it will continue to proactively transform the Indian industry's engagement in national development.

CII is a non-government, not-for-profit, industry-led, and industry-managed organisation, with about 9,100 members from the private and public sectors, including SMEs and MNCs, and an indirect membership of more than 300,000 enterprises from 288 national and regional sectoral industry bodies.

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

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

With the theme for 2020-21 as Building India for a New World: Lives, Livelihood, Growth, CII will work with government and the industry to bring back growth to the economy and mitigate the enormous human cost of the pandemic by protecting jobs and livelihood.

With 68 offices, including 10 centres of excellence in India and 9 overseas offices in Australia, China, Egypt, Germany, Indonesia, Singapore, the UAE, the UK, and the US, as well as institutional partnerships with 394 counterpart organisations in 133 countries, CII serves as a reference point for the Indian industry and the international business community.

Confederation of Indian Industry
(Northern Region) - Sub-regional Office
Plot No. 249-F, Sector-18, Udyog Vihar, Phase IV,
Gurugram - 122 015
T: +91-0124-4014073 • F: +91-0124-4014070
Email: ciinr@cii.in • Website: www.cii.in

End Notes

[1]Deloitte Report: "The Fourth Industrial Revolution – At the intersection of readiness and responsibility"

https://www2.deloitte.com/us/en/insights/deloitte-review/issue-22/industry-4-0-technology-manufacturing-revolution.html

[2]https://iottechnews.com/news/2019/jun/14/global-iot-spending-break-1-trillion-2023-fuelled-solid-consumer-and-commercial-adoption/

[3]https://iottechnews.com/news/2019/jul/18/idc-asia-pacific-will-spend-almost-400bn-internet-things-2023/

[4]https://www.globenewswire.com/news-release/2020/06/19/2050758/0/en/Industrial-IoT-IIoT-Market-Worth-263-4-billion-by-2027-Exclusive-Report-Covering-Pre-and-Post-COVID-19-Market-Analysis-and-Forecasts-by-Meticulous-Research.html

[5]https://www.bbc.com/news/science-environment-48283612

[6]https://www.interact-lighting.com/global/iot-insights/the-iot-and-climate-change

[7]https://economictimes.indiatimes.com/industry/energy/power/indias-renewable-energy-capacity-crosses-80gw-mark-r-k-singh/articleshow/70244364.cms

[8]https://www2.deloitte.com/us/en/insights/focus/industry-4-0/industry-4-0-business-models.html

[9]Mark Cotteleer and Tim Murphy, "Behavioral economics key to maximizing human-technology engagement in a digital supply chain," Supply Chain Navigator, October 2017. View in article

[10]https://www2.deloitte.com/global/en/pages/about-deloitte/topics/combating-covid-19-with-resilience.html#

https://www2.deloitte.com/us/en/insights/focus/cio-insider-business-insights/reimagining-the-technology-operating-model.html

https://www2.deloitte.com/us/en/insights/focus/industry-4-0/cocreation-accelerating-product-innovation.html

https://www2.deloitte.com/us/en/insights/focus/industry-4-0/industry-4-0-business-models.html

https://meity.gov.in/writereaddata/files/Revised-Draft-IoT-Policy_0.pdf

https://www.ltts.com/sites/default/files/news/2017-07/coe-iot-release-_news.pdf

https://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf

https://www.thehindubusinessline.com/info-tech/skill-development-govt-approves-rs436-crore-to-train-professionals-in-iot-ai-and-blockchain/article30338880.ece

https://meity.gov.in/content/innovation-promotion

https://sloanreview.mit.edu/article/demystifying-data-monetization/

https://www.livemint.com/industry/energy/india-plans-to-change-all-electricity-meters-to-prepaid-smart-meters-by-2022-1563331480075.html

https://www2.deloitte.com/content/dam/Deloitte/in/Documents/IMO/in-imo-annual-status-of-higher-education-in-states-and-UTs-2015-noexp.pdf

https://reports.weforum.org/industrial-internet-of-things/5-recommended-actions-for-stakeholders/?doing_wp_cron=1583318145.7489590644836425781250

See examples of telecom leveraging institutes for 5G research -https://telecom.economictimes.indiatimes.com/news/partner-led-approach-to-help-telcos-reduce-iot-deployment-cost-deloitte/72365607

[i]https://www2.deloitte.com/global/en/pages/risk/articles/covid-19-managing-supply-chain-risk-and-disruption.html#

[ii]https://niti.gov.in/writereaddata/files/Booklet%20of%20Synopsis%20-%20Aug%2022%20Final.pdf

Contacts

Deloitte Touche Tohmatsu India LLP

Ashvin Vellody
Partner
ashvinv@deloitte.com

Shridhar Kamath
Partner
shridharkamath@deloitte.com

Gautam Kapoor
Partner
gkapoor@DELOITTE.com

Antony Prashant
Partner
prantony@deloitte.com

Confederation of Indian Industry

Deepak Sidha
Deputy Director
deepak.sidha@cii.in

Acknowledgments

Shatanik Goswami
Monika Bagchi
Alankar Sain
Vineet Tyagi

Confederation of Indian Industry
125 Years - Since 1895

Published by Confederation of Indian Industry (CII).

Deloitte.