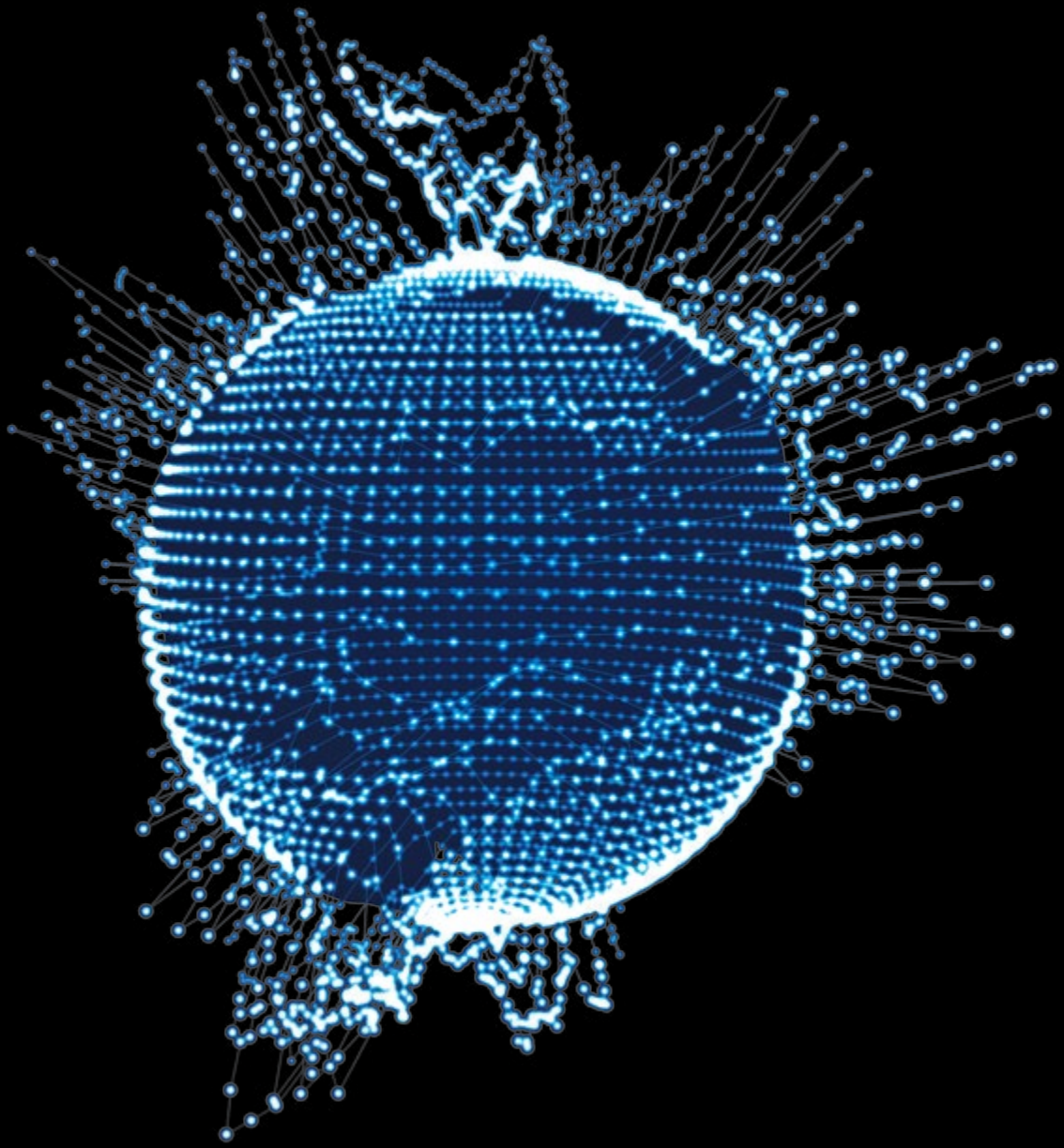
Deloitte.

Confederation of Indian Industry



Security and Privacy in the Digital World

November 2017

Contents

Foreword

Hemant Joshi

In the Digital and Interconnected world, there is an exponential growth of data, almost doubling every two years. The cumulative data generated so far in the world is less than the data that will be created in this year 2017. By 2020, 4 billion people are expected to be connected generating 50 trillion GB of data annually. This data has in fact led to the rise of cyber physical systems and is driving the business models helping organizations provide the relevant offerings to customers when they need it. With so many interconnected devices and huge amount of data at stake, the need for Cyber and Data security has reached levels seen never before in the history of internet era. The more the data with an organization, the more valuable the organization is for an attacker. According to analysts, security spending will continue to grow in 2017 when revenue is projected to reach $1.24 billion in India ($86.4 billion globally).

Organizations are evolving themselves from being product companies to technology companies. New technologies like Internet of Things (IoT), Artificial Intelligence (AI), Virtual Reality (VR), etc. are enabling businesses to look beyond the conventional operating models and explore new horizons. Due to convergence, the boundaries differentiating organizations and sectors are blurring as technology becomes an enabler to drive customer experience and hence revenues.

The cyber-attacks, including the WannaCry ransomware attacks, Dyn DDoS and others, on the biggest media company, UK's biggest telecom company, Indian banks, Heathrow Airport, etc. provides testimony to the fact that organizations are constantly under threat. The data leaked included personal information about employees, clients, e-mails between employees, information about executive salaries at the company, and other sensitive information. Such is the scenario today that the world is moving away from physical warfare towards digital warfare. Hence, organizations and countries need to have robust security and privacy frameworks as newer threats evolve in the digital world.

In 2017 and beyond, most enterprises in India would embark on digital transformation programs in order to fine tune existing business and operational efficiencies, improve productivity and performance, and enhance reliability. The new digital business environment comes with unprecedented risks that go beyond IT operations, encompassing the enterprise, partners, in fact its entire supply chain and ecosystem. More and more organizations are now using or offering technological services through means beyond their control (for example use of public cloud).

These are exciting times for all stakeholders of the digital ecosystem. The organizations which embrace the change and adopt measures to ensure security of data will be better placed for the future. All stakeholders of the digital ecosystem (individuals, organizations and government) need to build security as an integral part of their DNA. The need of the hour is for a cohesive approach to build a secure ecosystem which facilitates business growth and enhances customer experience.

Message from Confederation of Indian Industry

Umang Das
Summit Chairman

Cyber security has become the backbone of the Government, Industries and enterprises now. Geographical distances or political boundaries do not matter because cyber-attacks can be launched from any corner of the world. With the move towards a digital economy, increasing amount of consumer and citizen data will be stored digitally and a large number of transactions will be carried out online, by companies, individuals as well as government departments. One of the biggest reasons behind this is the limited awareness of the impact and importance of cyber security currently.

Cyber threat intelligence entails many things, such as understanding your infrastructure, your employees and your information, but the bottom line is it provides actionable information, say experts during a recent fireside chat program entitled "Intelligence-Driven Security."

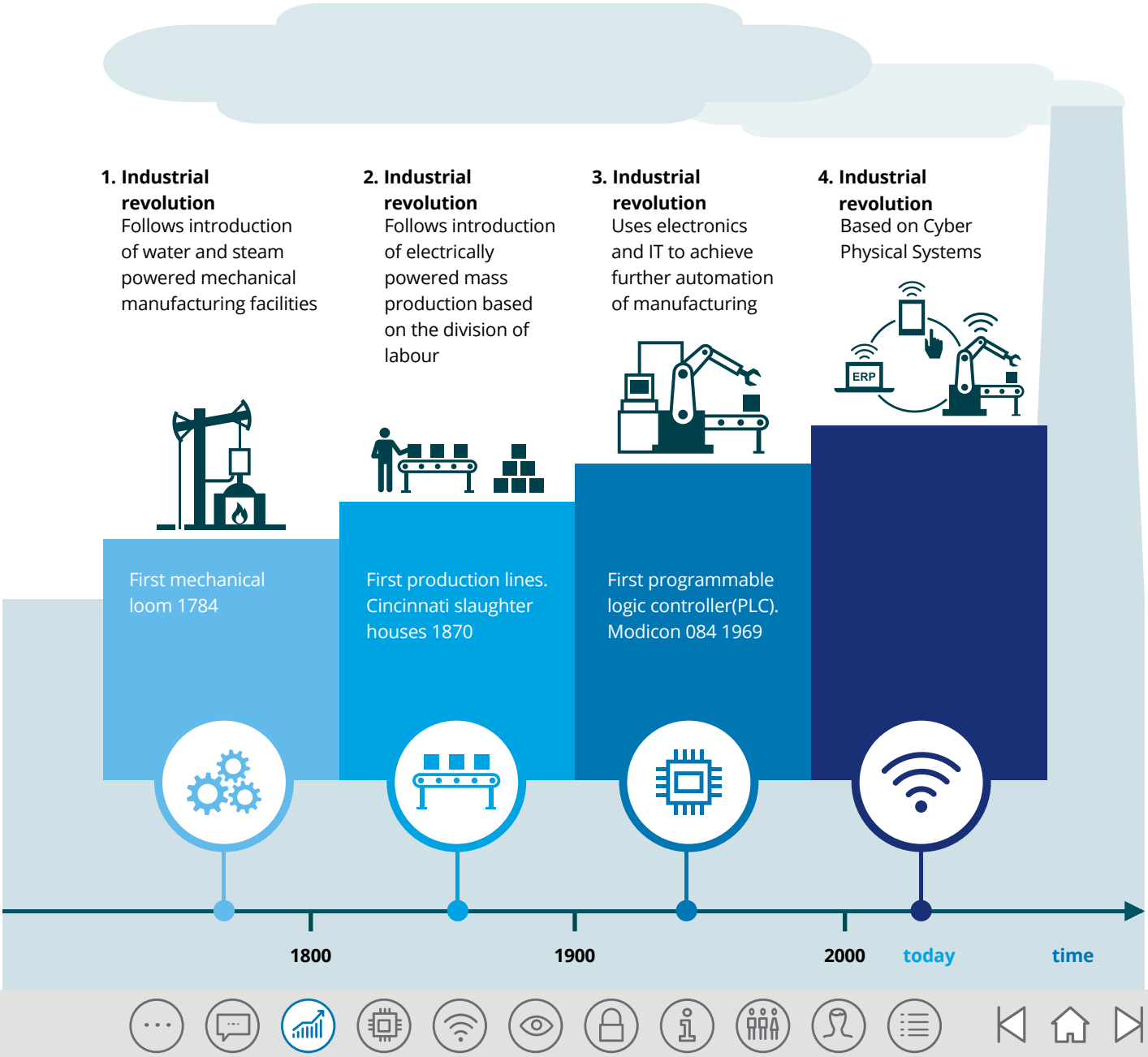
As such, there is limited awareness of the need for specialized and customized industry-specific cyber security measures which are significantly different from IT security and need to be adapted by the industry.

One of the biggest misconceptions about cyber security is that cyber-attacks are restricted to the financial services and banking sector. It is important to note that industrial companies are equally vulnerable. At the same time, it has become clear that conventional IT systems and firewalls are increasingly becoming ineffective in preventing sophisticated hackers from creating havoc.

What we need is national level effort to build skills in this very sophisticated area of technology to either develop such hi-tech equipment ourselves, or atleast be capable of critically inspecting them before these are deployed in critical infrastructure and critical industry sectors and today's Summit, focused on understanding the nature of the evolving cyber landscape and how to address it. IT leaders from across Industry, Government would discuss the key issues that agencies need to address in the coming years—and the technologies and strategies that will be critical to that effort.

1. Securing growth for business in a digitally enabled ecosystem

The world we live in has evolved over the last few years and this has been made possible due to the rapid advancement of technology in each field. This change is in fact driving the next industrial revolution – a phenomenon now termed as Industry 4.0. The major driver for the advent of Industry 4.0 are the cyber physical systems. Integrating the DNA of Industry 4.0 in its service offerings, Deloitte Digital is working actively towards building a secure digital enterprise. These offerings are even more important as organizations are also evolving from being product companies to technology companies. The boundaries differentiating organizations and sectors are blurring as technology becomes the key enabler and driver. Traditional business models have given way to new ways of working in the digital world. For example, light equipment manufacturing companies are now offering lighting as a solution to city municipal corporations. The operating model is shifting from capital expenditure based to operating expenditure based.



With the new Digital and Interconnected world, the data that companies have access to is increasing enormously. It is this data which is driving the business models helping organizations provide the relevant offerings to customers when they need it. Such initiatives are being used by organizations to improve customer experience and use it as a differentiating factor. As one of the leading industrialist of the country rightly put it, "Data is the new oil". As technology evolves even further, this data shall become even more important and sought after.

By 2020, the world is expected to change[1]

This is a paradigm shift and with so many interconnected devices and huge amount of data, the need for Cyber and Data security has reached high levels like never before in the history of internet era. There are even more avenues which are available to an attacker to disrupt an organization. The world is moving away from physical warfare and now moving towards digital warfare. Hence, organizations and countries need to have robust security and privacy frameworks as newer threats evolve in the digital world. For organizations to grow, adequate security measures need to be put in so as to prevent any damage. These safeguards need to be incorporated not just in the organization under question but across all entities which form part of the value chain. The digital infrastructure thus secured should be reviewed and upgraded regularly to ensure protection against newer threats.

A telecom operator is one of the few entities which has access to a large amount of data of the customer. This data is critical for enhancing B2B2C models for the growth of telecom industry in India. This data is also important for various other sectors like insurance, banking, etc. which are governed by their own regulatory policies. As is the case with the new digital world where business models are converging and organizations are getting into symbiotic relationships with each other, the regulatory framework governing these sectors also needs to converge. A collective approach is required with various regulatory bodies like RBI, IRDAI, and the likes in defining a common executable policy framework that is acceptable to all stakeholders. By doing so it will boost the Digital India campaign in New India paving way for new business models, ecosystems, and economy.

Though data privacy is covered under the IT Act, the scope now needs to be expanded to include all players in the telecom ecosystem, importantly Apps (like Skype, Google, WhatsApp, etc.), App developers, Communications Service Providers (CSP), Internet Service Provider (ISP), Device manufacturers etc. As a principle, the framework should ensure that the customer is aware of the ways and means in which their data is being used. However in scenarios where customer privacy is not getting impacted, the data owner shouldn't be restricted from using the data for any business decision making/modeling.

In 2017 and beyond, most enterprises in India would embark on digital transformation programs in order to fine -tune existing business and operational efficiencies, improve productivity and performance, and enhance reliability. The new digital business environment comes with unprecedented risks that go beyond IT operations, encompassing the enterprise, partners, in fact its ecosystem. More and more organizations are now using or offering technological services through means beyond their control (for example use of public cloud). As businesses grow while embarking upon their digital journey, they also need to implement appropriate levels of risks and controls to safeguard the data and protect the ecosystem.

2. Technology driving consolidation and convergence

The advent of exponential technologies like RPA, Artificial Intelligence (AI), Machine Learning, Internet of Things (IoT), Advanced Analytics, Cloud Computing, Big Data, advancements in technologies like 3D manufacturing sensor technologies, industrial robots, drones and autonomous vehicles has far greater "combinatorial effect" than the impact of deploying these technologies in silos. The confluence and ever-wider availability of these technologies promise to fundamentally alter the way we live, process, work and interact–a development that has been termed as Industry 4.0 and today we are already at the cusp of a major digital transformation across industries.

As a result of these digital exponential technologies, industries are facing new digital business realities that have redefined traditional industry and market boundaries and have led to Industry Convergence, a growth strategy focused on innovative cross industry value experiences that has created new possibilities for organizations to pursue business opportunities outside industry sectors they previously conducted the majority of their business. Blurred lines between industries have shifted the focus away from individual products to cross-industry value experiences which are based on digital business principles.

Successful organizations have started delivering the cross-industry value experiences by developing their offerings targeting multiple industries and by partnering with right players from other industries rather than trying to grow alone within their own industries and competing on cost for market share in a shrinking market. According to Gartner, by 2020, the top industry-leading organizations will generate 15% of their revenue from digital cross-industry value experiences that are the result of industry convergence.

In the wake of the Digital Revolution that is taking place, let us analyze some of the industries and their evolving ecosystems to understand the Industry convergence, the opportunities that arise from this, and the underlying technologies driving this.

Future Industry Digital Ecosystems	Digital Technologies Disrupting/Providing Growth Opportunities in the Industry	Converging Industries
Connected Health Care	IoT, Analytics, Cloud, Wearables	Healthcare, Fitness, Pharmaceutical, Technology, Apparel, Telecom
Connected Automobile	IoT, Cloud, Big Data, Cognitive Automation	Automobiles, Technology, Energy and Utilities, Telecom, Insurance
Smart Home	IoT, Analytics, Cloud, Cognitive Automation	Technology, Consumer Electronic Goods, Energy and Utilities, Telecom, Healthcare

1.1. Connected Healthcare

This involves the convergence of Healthcare industry, Technology, Digital Media, Pharma companies, Telecom and Apparel industry to deliver good quality healthcare at low costs and in a more accessible manner. Some of the opportunities include Patient Alerts for monitoring Treatment adherence, Remote Health status monitoring and remote Diagnosis, Contact lenses to monitor Glucose levels, Heart rate monitoring patch, Smart pills monitoring medication behaviors and body responses, Wrist band to monitor BP, Heartbeat, and Calories burnt and so on.[2]

1.2. Connected Automobile

This has forced Automobile manufacturers to shift focus towards services and User experiences in the vehicle which has in turn forced them to venture into other industries or identify partners from other industries. Some of the opportunities include Real Time Navigation, Remote Vehicle Diagnostics, Predictive Maintenance, Mobile Device Integration into Automobiles to provide overall customer experience, New in-vehicle user experience (UX) and user interface (UI) scenarios like gesture control, conversational Interface, AR display and Self-driving vehicles that can operate without human intervention in most roadways situations or conditions.[3]

1.3. Smart Home

The concept has attracted players from across industries like Healthcare, Power Utilities, Consumer Electronics Goods and Technology. Some of the opportunities companies are exploring include Automated Heating control systems, Automated Energy monitoring and control systems, Smart Entertainment, Camera surveillance, Alarm systems, Assistance for seniors, Emergency call and Remote surveillance.[4]

In the wake of the Digital Revolution that is taking place in every industry, industries have been forced to consider one of the below options to stay relevant and compete:

- Venture into an industry which is significantly different from the current operating industry
- Partner with a player in a different industry
- Acquire a player in a different industry

Below are some of the examples that highlight this trend:

Nike, traditionally a sports apparel manufacturer with primary focus on Shoes, has ventured into Healthcare/ Fitness industry by integrating Pressure sensors, Fitness App, Band, Accelerator programs with its products (shoes).

Caterpillar acquired Yard Club, a start-up founded to make more efficient use of construction and other heavy equipment.

General Motors Fleet and AT&T offers customers with GM Fleet corporate accounts an opportunity to activate OnStar 4G LTE Wi-Fi hotspots, in millions of cars, trucks and crossovers with the ability to share unlimited data and receive simplified invoices with centralized billing which could transform the in-vehicle experience for business customers through high-speed 4G LTE internet service. 5 million 4G LTE-equipped GM vehicles are on the road as of 2017. GM customers have used more than 14 million gigabytes of data since the launch of OnStar 4G LTE, equivalent to sending and receiving nearly 140 billion emails with attachments.[5]

Waymo, a company spun out of Google, is a self-driving technology company working on making Driverless Cars, a reality.

3. Telecom aiding the convergence

Telecom ecosystem has evolved over the years and is much more matured today where there is some degree of convergence at all three critical layers: Network, Device and Services. In order to move towards the path of "True Convergence" Telco's needs to seize the opportunity that Industry 4.0 presents and position themselves as corner stone for the next wave of digital transformation. We're already witnessing the growth in information and money flowing through the global economy and it is mindboggling.

Global landscape of goods, services and finance could increase three-fold from $26 trillion in 2012 to more than $80 trillion in 2025. To put these figures in perspective, the total value of these flows increased only 1.5 times in the 20 years between 1990 and 2012. Global broadband speeds are increasing at 20% a year (rates of 1,000 Mbps are now becoming a reality), opening tremendous possibilities for businesses and society. The importance of the telecom industry's role is only likely to grow as companies across industries integrate digital exponential technologies to drive their new business models and thus increase the importance of the underlying network enormously.

Over the same period, the number of connected devices, which enable and drive business models in the IoT, could reach 30 billion. New technological initiatives such as drones and autonomous vehicles will depend heavily on reliable and secure connectivity. We are already at a stage where networks going down could put entire businesses and perhaps human lives at risk.

For example, MIT researchers have modelled a system of autonomous vehicles and reducing wait times by an estimated 80 per cent or more. But that system requires vehicles to be connected with a common traffic management system, and further requires a network latency much lower than what is currently provided by 4G networks.

The era of ecosystems and the need for data security

With the emergence of ecosystems, IT-OT interfaces have increased manifold exposing the network to vulnerable points, making security another critical issue that needs to be addressed. For example, an increasingly connected and intelligent infrastructure would be exposed to security threats as the interfaces increase exposing large amounts of data to vulnerabilities.

Major wireless carriers and infrastructure solution providers have developed partnerships with automotive OEMs, country governments, and technology providers to support the development of standards for autonomous transport. Tier-1 telecom companies in the United States are investing billions of dollars to build high-speed, next-generation broadband infrastructure, even as they work closely with regulators to help accelerate the rollout of fifth-generation wireless technology (5G).

Telecom companies can also aid in providing highly personalized services, such as behaviour-based, contextual and mood-based advertising, connecting devices at home. The day is not far when replenishment orders could be placed automatically for medicines and groceries simply because your refrigerators would be connected to the grocery aggregator.

The following table sums up the key relationships that recent times have seen or are about to see:

Figure 1: Emerging ecosystems of industries with telecom at the centre of connectivity

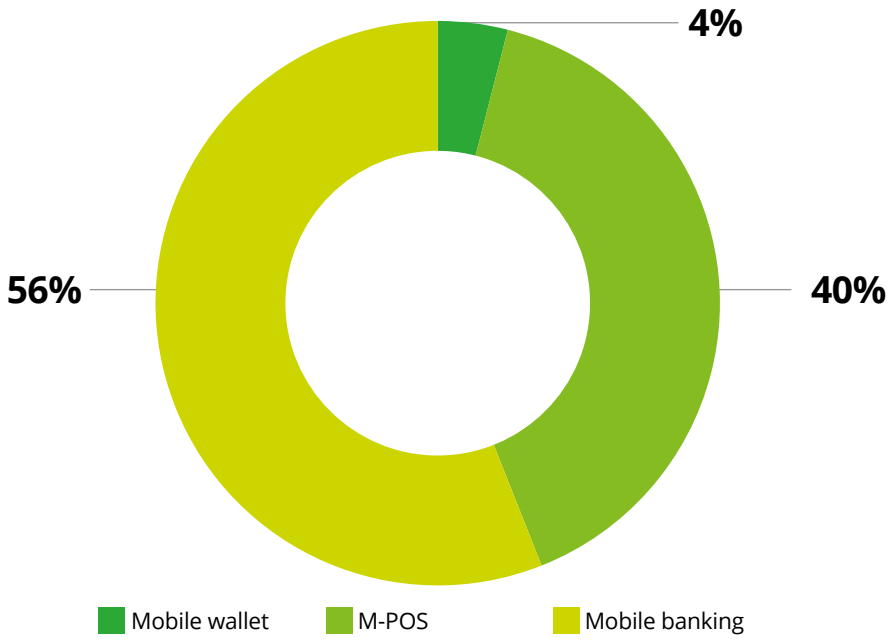
Industries	Organizations	Purpose
Oil & Gas , Telecom	HPCL, Airtel	Airtel Payments Bank customers would be able to access a range of convenient banking services
IT, Telecom	IBM	Exploring partnerships with telcos around network functions virtualization (NFV) technology
	Google, Airtel, SK Telecom	Bring Indian telecom operators on board Google's software defined networking (SDN)-based platform
Consumer and Industrial Products, Telecom	LG, Telecom players	Build smart appliance equipped with features such as LG HomeChat and SmartThinQ that enable consumers to control and operate home appliances through smartphones
	Bharti Airtel, Ecommerce players, mobile handset vendors	Three-way agreements to offer attractive data plans when a person buys a handset online
Media, Telecom	Bharti Airtel, OTT players like Ditto TV, ErosNow, SonyLIV and Hooq	Live TV and video on demand services
	Ericsson, Bharti Airtel	Ericsson has already deployed a suite of optimization solutions for Bharti Airtel in OTT space

Source: Deloitte Analysis

Such partnerships would involve a huge amount of data along with multiple interfaces, which could be tapped for data breaches. It is here, that cyber security would be of utmost importance to ensure data privacy for the customer.
To ensure seamless purchase of services across the ecosystem, mobile and digital payments will play a key role but along with them, data security will take the centre stage.

The changing face of the relationship of Telcos and Financial services
During the last few years, the three key offerings, which have emerged in the digital mobile economy, are mobile wallet, m-PoS, and mobile banking. FY 2016 saw the rise in digital economy with mobile payments becoming the order of the day and providers such as Paytm and MobiKwik crossing millions of accounts. During FY 2016, the total transaction volume of the m-payment in India was 2.9 billion; it is expected to grow at a CAGR of 132% during FY 2016-FY 2022, and reach around 460 billion by the end of 2022.[6]

Figure 2: Mobile payment by segment, FY 2017



Note: Breakup is shown in terms of transaction value
Source: RNCOS

Growth drivers for these transactions are the exponential rise of mobile internet users, increasing usage of smartphones, growth of e-commerce transactions, which have in turn aided in the growth of mobile payments. But, the news of data leaks, user account information being stolen, payment details being at the risk have been doing the rounds as well across the globe. A prominent food delivery aggregator in India reported user data being compromised with 17 million users' data up for sale on the dark web marketplace.[7]

It is at this point that customer experience suffers, with the fear of filling card information online creeping in, and ultimately losing out in the seamlessness of the transactions of the ecosystem. Telcos can play a significant role and become the backbone of the digital economy by providing the extra layer of security in transactions.

The future

While the availability of inexpensive smartphones have enabled consumers across the country to become part of the digital ecosystem, even in Tier II an Tier III cities, the real game changer has been the competitive pricing and internet services from telecom companies, which have been trying to increase their customer base and improve Customer Experience (CX). The future holds two key themes, which will emerge, and further improve the overall CX.

Single point of authentication - TRAI Chairman R.S. Sharma was recently quoted as saying, "My vision is that I should be able to access any public wi-fi, paid or free, by a single authentication at one point, across hotspots, till I reset it". The day is not far when this would become a reality in the Indian landscape. Single authentication will tend to improve the overall customer experience and decrease the touchpoints in the customer journey.

To support Mobile based authentication and identity, GSMA has initiated a new concept called “Mobile Connect”. GSMA Mobile Connect is a simple and convenient solution providing users with universal secure and privacy-centric authentication services, facilitated by mobile operators leveraging on their inherent security of mobile networks and SIM. It is designed to position mobile operators as trusted providers of – Authentication, Identity and Attribute brokerage services.

In 2015, all major Indian mobile operators and GSMA formed a multi-operator Mobile Connect industry consortium and successfully launched the services in July 2016. They are already working with a few digital merchants in the ecommerce and travel space and are also in advanced discussions with leading banks to integrate Mobile Connect. The Mobile Connect deployment can be expanded in a number of directions with support from Government and regulatory bodies which will enhance the security and privacy aspects.[8]

In view of the above, the next decade of digitization will look markedly different from the past and telecom companies will need to be well-prepared to take advantage of the sweeping transformation taking place in consumer lives, enterprises and the broader economy.[9]

4. Getting ready for the future – nurturing talent

With a more complex and intertwined global technology environment, the number of digital risks facing organizations today continues to multiply. Risks in the digital business environment affect the entire ecosystem and are not restricted to IT alone. More and more organizations are now using or offering technological services through means which they do not own or control (for example software as a service or use of public cloud). Whether it is regulation or use of new digital platforms, the complexity of risks requires an entirely new skillset. With the evolving technological models, the risks and threats are also increasing and so are the budgets required to meet these threats and mitigate the risks. Organizations now have to choose what are the risks and their impacts which they can live with and the ones which need to be addressed on priority.

The security professionals responsible for the traditional Information Security portfolio of an organization have to start looking beyond the conventional IT and shall now have to address needs ranging from IT to Operational Technology (OT) to Internet of Things (IoT) to partner management. These professionals will not only be required to understand IT technologies and the modalities of mitigating risks associated with it, they shall also have to learn the ways and means to address the risks and challenges posed in the new environment – some known and some unknown. According to Gartner, by 2020, 60% of the digital businesses are expected to suffer major service failures due to the inability of its security teams to manage digital risk.

The new breed of security individuals shall have to understand Technology, Business processes and the implications of implementing the digital initiatives. These individuals shall be valued on the basis of their knowledge and understanding of the business and its processes rather than just their knowledge of the IT systems and the security protocols needed to safeguard the organization.[10]

These new business models demand specialised skillsets and more importantly a flexible mind set of the individual—a combination of which is very difficult and rare. The shortage of resources with appropriate skills and awareness is now starting to impact organizations and the problem is only expected to aggravate as time progresses. There are two immediate solutions available with organizations as a potential solution to this problem:

01. Develop talent in-house through specialized and targeted training programs for existing professionals. These programs can range from workshops to certification programs to full time executive programs for the nominated employees. These programs should be so designed that they offer the opportunity for continual learning for the professionals. The programs can be customized for the organization on the basis of the existing risk management framework and the roadmap going forward.
02. Explore avenues of external hiring on the basis of the desired skillsets. External hiring can be in terms of either contractual or full time resources depending upon the budgets allocated and the criticality of the work to be allocated. Since the demand for digital skillsets and more importantly for skillsets pertaining to Digital Risk Management is growing at a fast pace, the availability of such resources at a budget suitable to the organization is proving to be a major hurdle.

A long term measure which can be taken by organizations to ensure availability of the right resources with the right skillsets is to tie up with educational institutes and universities and develop content which is specific to the industry and the organization. This can be done by an individual organization or a pool of organizations in the same industry. Such centres of excellence can serve as breeding grounds and test labs for future innovations and developments in this field. This will ensure availability of resources and professionals which meet the requirements of the industry and are fit to deliver from day one of them joining the organization. The courses developed can also be then used by the organization for its internal training programs and certifications for enhancing digital talent.

Having strategic partnerships with an educational institute will not only help availability of the right professionals with the right skillsets, but will also enable the academia get an insight into the workings of the professional world. This symbiotic relationship can aid in developing the overall ecosystem and shall also work towards the Government's Skill India initiative. The Government could ideally promote such partnerships and reward organizations which take such initiatives so that it is a win–win situation for all stakeholders.

In conclusion, the ecosystem is changing and the new digitally converged world requires skillsets which are specific to the ecosystem. The set of challenges and risks associated are also different from what organizations are used to dealing with and hence the need of the hour is for professionals to embrace new knowledge and new skills. The security professionals responsible for the traditional Information Security portfolio of an organization have to start looking beyond the conventional IT and shall now have to address needs ranging from IT to Operational Technology (OT) to Internet of Things (IoT) to partner management. Beyond Technology, they will also have to understand the business strategy and the entire ecosystem restricted not just to Technology. These new set of individuals shall be valued for their understanding of both business and technology and shall drive the Enterprise risk portfolio approach.

To ensure availability of the right skillsets to take up the new challenges, organizations shall have to look at both internal and external professionals. In their quest for such skillsets, organizations shall have to move beyond the conventional operating model and look at strategic partnerships with educational institutes which shall help provide a stream of resources with the right skillsets required by them.

5. Providing a secure digital experience

With the huge amount of data that is now available from various digital channels, it is very important for organizations to get an accurate insight and assessment into various digital risk domains. Organizations are however still struggling with the complexity which comes with the deployment of digital initiatives despite having an intent and a defined digital vision. Some of the key risks which an organization might face in their digital journey are:

01. Having the appropriate digital strategy and supporting architecture.
02. Non usability of the existing application stack and infrastructure to enable the digital journey.
03. Piecemeal approach or a staggered deployment of digital initiatives across the organization leading to issues in the interworking between digital and legacy systems.
04. Unfamiliarity and reluctance towards the use of digital technologies by employees and partners to perform tasks to support the organization's operations.
05. Evolving regulatory and compliance requirements leading to organizations having to adopt newer controls and implement systems to support the digital ecosystem.
06. Usage of newer and shared technologies (like cloud, software as a service, etc.) means limited controls available with the organization hence leading to more secure systems to be put in place.
07. Processes not aligned to support the digital ecosystem.

Coming up with a comprehensive approach to counter the risks associated with a digital ecosystem is of utmost importance for an organization. While data security is one of the key risks which need to be mitigated, , organizations need to look beyond the conventional risks which they have been used to so far in the digital world. For example, as organizations and business models become more and more dependent upon data and its volume increases, the requirement for having resilient systems and technologies which support faster processing of data increases. Organizations need to be prepared and factor in the associated risks in such scenarios.

Insights into the risks which might impact an organization can be gained from various sources:

01. Social media and public forums: Social, mobile, web and other public domains provide a vast amount of information as to what are the kind of threats and risks facing an organization. Solutions then have to be tailored specific to the kind of threat facing an organization. Regular monitoring of channels beyond the conventional ones can also provide pointers to various activities which can cause potential damage to the organization.

02. Paid insights: There are various tools and companies which provide details on what is the sentiment of the masses on various social media channels. Twitter, Facebook, and other such technology companies provide various analytics when subscribed to for these services.

03. Insights from data internal to the organization: Attacks on organization's internal assets like application servers, interconnection links etc. can be pointers to a bigger activity targeted towards the organization's public assets. For example, usage trend of diesel in generator sets can point to an increase in power outages in an area meaning that cold storage facilities should either brace for increased operating expenses or work towards optimizing procurements to reduce dependence on generators.

Collation and interconnection of the information received from various channels is very important for any organization. In today's interconnected world, an event impacting one industry/ sector can have an impact on multiple other sectors. For example, if the internet services of the service provider aren't working in an area and there is widespread chatter on social media on this, app based food delivery or cab services would also start getting impacted as customers wouldn't be able to avail their services. Organizations need to come up with mitigation plans on real time basis such insights.

Some of the additional measures which need to be taken for risk management:

01. **Third party data sources –** Ensure that all the stakeholders and the parties involved are following the correct data format as prescribed by the risk and security framework to draw meaningful insights from different data sources.
02. **Information from conventional and non-digital channels:** Information Information captured for multiple purposes can provide insights into impending threats and risks which an organization could face – both internal and external.
03. **One size doesn't fit all:** A solution successfully deployed at one organization might not be successful at the second organization as the rules of operation and the risk taking appetite differs from organization to organization.
04. **New technologies give new insights:** Using new technologies can lead to timely actions being undertaken. For example, wearable devices strapped onto traffic policemen can, on a real time basis, monitor their vital body statistics. On the basis of the information received timely actions like medical aid can be provided.

At the end of the day, all insights provided should be corroborated by individuals with relevant experience so as to ensure the right decisions are taken.

As organizations evolve so shall the amount of data being generated and used by them. This data deluge could lead to organizations facing newer threats for which they shall have to adopt advanced security practices or leverage professional services from firms specializing in the relevant field. This would mean not just protecting the organization from unauthorized access but also ensuring that adequate measures are in place to protect the privacy of the individual from being leaked outside of the organization. One of the implications could also be to implement a risk framework to build a secure organization with the right people, processes and technologies. The risk framework shall include not just the organization but all other relevant stakeholders which have a bearing on the value chain and impact the ecosystem.

About CII

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

CII is a non-government, not-for-profit, industry-led and industry-managed organization, playing a proactive role in India's development process. Founded in 1895, India's premier business association has over 8,300 members, from the private as well as public sectors, including SMEs and MNCs, and an indirect membership of over 200,000 enterprises from around 250 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.

The CII theme for 2017-18, **India Together: Inclusive. Ahead.** Responsible emphasizes Industry's role in partnering Government to accelerate India's growth and development. The focus will be on key enablers such as job creation; skill development and training; affirmative action; women parity; new models of development; sustainability; corporate social responsibility, governance and transparency.

With 66 offices, including 9 Centres of Excellence, in India, and 10 overseas offices in Australia, Bahrain, China, Egypt, France, Germany, Singapore, South Africa, UK, and USA, as well as institutional partnerships with 344 counterpart organizations in 129 countries, CII serves as a reference point for Indian industry and the international business community.

Acknowledgements

Strategic direction

Hemant Joshi
Shree Parthasarathy
Vishal Jain

Deepak Sidha
Deputy Director
CII

Key contributors

Prakash Sayini
Gaurav Khera
Titikhya Dey
Ambika Bahadur

Contacts

Confederation of Indian Industry
Plot No. 249-F, Sector-18, Udyog Vihar,
Phase IV, Gurgaon - 122 015
T: +91-0124-4014073
F: +91-0124-4014070
E: ciinr@cii.in; deepak.sidha@cii.in
W: www.cii.in

Deloitte
Deloitte Touche Tohmatsu India LLP
706, B Wing
ICC Trade Towers
Senapati Bapat Road
Pune - 411016, Maharashtra
Tel: +91 (0)20 66244600
Email: inideas-tmt@deloitte.com
www2.deloitte.com/in

References

[1]Digital Transformation Initiative, World Economic Forum, Jan 2017:
http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/white-paper-dti-2017-telecommunications.pdf

[2]Connected Health, Deloitte Centre for Health Solutions:
https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/life-sciences-health-care/deloitte-uk-connected-health.pdf

[3]Connected vehicles enter the mainstream, Deloitte:
https://www2.deloitte.com/us/en/pages/manufacturing/articles/connected-vehicles-enter-the-mainstream.html

Caterpillar acquired Yard Club, a marketplace for construction equipment, May 2017, https://techcrunch.com/2017/05/05/caterpillar-yard-club-acquisition/

[4]Switch on to the connected home: The Deloitte Consumer Review, July 2016:
https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-16.pdf

[5]GM First to Offer New AT&T Connected Car Data Plans for Business Customers, May 2017:
http://media.gm.com/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2017/may/0516-data-plans.html

[6]MWallet: Scenario Post demonetisation, RNCOS

[7]Zomato hacked, 17 million users' data up for sale on dark web marketplace, May 2017: http://www.livemint.com/Companies/rZYbQfeFDTvWvs7vUPIqFP/Zomatos-17-million-accounts-hacked-data- sold-on-Dark-Web-m.html

[8]Connecting the future of mobility, Feb 2017, DU Press:
https://dupress.deloitte.com/dup-us-en/focus/future-of-mobility/role-of-telecommunications-in-new-mobility-ecosystem.html#endnote-7

[9]Digital Transformation Initiative, World Economic Forum:
http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/dti-telecommunications-industry-white-paper.pdf

[10]Create a Digital Risk Officer Role in your organization, Gartner, May 2016: https://www.gartner.com/doc/3323317/create-digital-risk-officer-role
Managing Risk and Security at the speed of Digital Business, Gartner, August 2017: https://www.gartner.com/doc/reprints?ct=160408&id=1-333TSGU&st=sb

Published by Confederation of Indian Industry (CII).

Deloitte.