The next normal in cybersecurity

ASSOCHAM – EY report

February 2020

ASSOCHAM
Celebrating 100 Years

EY
Building a better working world

Content

President Foreword

The rapid pace of technology assimilation with billions of connected people and machines is accelerating the spread of threats. Therefore, the security of our cyberspace is now paramount. Cyber security works as the interface of technology, privacy and law. Delivering on the Hon'ble Prime Minister Modi's vision of Digital India, will require us to work across these domains and coordinate across a connected world.

Cyberattacks around the world are occurring at a greater frequency and intensity. Not only individuals but also businesses and governments are being increasingly targeted. The profile and motivation of cyber attackers is fast changing. A new breed of cybercriminals has now emerged, whose main aim is not just financial gains, but also causing disruption and chaos to businesses in particular and the nation at large.

With every passing year, cyberattacks continue to escalate in frequency and severity. As per a media report, nearly 3.9 lakh cyber attacks were reported to Cert-in in 2019, as compared to 2.08 lakh such incidents in 2018.

ASSOCHAM is committed to creating more awareness about the cyber-related issues.

We convey our very best wished for the success of the INDISEC 2020 Summit.

With best regards,

Dr. Niranjan Hiranandani
President, ASSOCHAM

Message

Cyber Security is now viewed as an integral part of culture and strategy of the organization, increasing its earlier ambit from a function of information technology or information security alone. It is reflected in each and every facet of the organization, right from the strategy to the behaviour of an individual employee. Such an integrated cybersecurity vision brings the organization's functions and stakeholders together towards the larger goal.

The Digital India program of the Government is leading a very important role in the economic, demographic and social transformation of the country. The goal of connectivity for all – leading to rapid expansion of digital fiber links connecting the nation; creation of digital identity – enabling every citizen to utilize services online; and financial inclusion – leading to operationalization of banking facility over mobiles for millions can only be met if there is a secure cyberspace to transact in.

We, at ASSOCHAM, have been discussing and deliberating with the concerned authorities and stakeholders about the need for security compliance and a legal system for effectively dealing with internal and external security threats.

ASSOCHAM is committed to creating more awareness about these issues and this background paper jointly prepared by EY and ASSOCHAM is a step in this direction. We congratulate the team for their efforts.

Our best wishes on this occasion for the success of the INDISEC 2020 with the hope that the Summit provides more insights into the emerging security challenges and their appropriate solutions for further securing the Country from such crimes.

Deepak Sood
Secretary General, ASSOCHAM

Technology continues to be embedded deep inside an organization's DNA and the way they service their customers.

However, the rapid emergence and adoption of new technology is riddled with significant challenges and disruption. While organizations understand the benefits of technology, they do not feel equipped to understand the associated risks and the measures required to mitigate the same. Thus, information security professionals have an unparalleled opportunity to act as agents of change by offering pre-emptive ways to mitigate risk and become key enablers of strategic transformation.

To keep up with the technology evolution it is imperative that the security function build strong relationships with business functions in order to get security considerations involved much earlier in new initiatives and in the transformation process. This will not only encourage a culture of security by design but will also enable enhanced allocation of resources consummate with organization's security needs.

This report presents a view on the complexities of the cyber ecosystem associated with four such emerging areas - cloud, 5G, Operational Technology (OT) and data privacy - which are being embraced increasingly by organizations and also defining the next decade for cybersecurity.

Murali Rao
Leader and Partner Cyber, Ernst & Young Associate LLP

Foreword

Executive Summary

The existing cyber ecosystem is becoming more complex and cybersecurity is one of the most discussed areas in organizations across the globe and in India. The scope of discussion needs to go beyond the existing services to new emerging technologies in the industry.

The objective of the paper is to help organizations understand the security risks for four evolving areas, decode the emerging trends and provide pointers for Chief information security officers (CISOs) to stay ahead of the threats.

Cloud

OT

5G

Data privacy

The influence of data intensive technologies like 5G and the cloud is rapidly extending the attack surfaces and increasing the possibility of organizations being hacked/attacked. Globally, currently more than 90%[1] of enterprises use cloud services and yet 67%[1] of security teams complain about the lack of visibility into their cloud infrastructure, security and compliance.

Misconfiguration of cloud resources remains the number one cause for cloud attacks.

Further as businesses move towards digital transformation, protecting the converged physical assets is becoming increasingly challenging. Industrial control systems (ICS) and Internet of Thing (IoT) devices are becoming easy targets of unauthorized access, modification, use, destruction and/or disruption. And in all this data privacy and personal data protection has evolved from being added bonuses to becoming key business imperatives. They are taking center stage and have now become a boardroom agenda.

In 2020, companies need a deeper security strategy for each of these four areas as cyber security is all about being prepared. In the sections below we will take a focused look at each of these technology evolutions and consider few leading practices being adopted by organizations to secure initiatives leveraging the same.

[1] Checkpoint , 2020 Cyber Security Report

Cloud

1

Cloud

Moving data to the cloud introduces new attack-surfaces, threats and challenges, so CISO of the organizations need to approach security in a new way.

Organizations typically have a mix of traditional IT and cloud services, so security solutions need to protect both. The security controls in place for the data center may not be suitable for new challenges introduced in the cloud. Big data, the new skills required of security teams and compliance and regulatory requirements all add to the complexity and cost of cloud security solutions.

The good news is that there are security solutions available to address the challenges. Ideally, a solution should minimize the load on the security team, as well as the training time required to support the solution. It also needs to address the new cloud security threats, while still protecting the legacy systems. Understanding the differences between cloud security and traditional security is key to finding the right security solution.

Cloud and traditional IT environments need protection against many of the same threats. Even though the threats may be the same, new solutions are needed to protect resources in the cloud.

1 **Containers, microservices and serverless**

Applications in the cloud often run serverless, as microservices, or in containers. Traditional security solutions are not equipped to handle these newer technologies. Threats can and often do go undetected.

2 **Elastic scalability**

The cloud is dynamic and elastic in nature. The frequent, sudden and hyperscale changes seen in the cloud would cripple many traditional security solutions.

3 **Hybrid and multi-cloud**

Another unique challenge is hybrid and multi-cloud architectures. Monitoring and analyzing of traffic traversing multiple clouds from different providers is difficult with on-premises security solutions.

Some of the new threats to adopting cloud services include:

It makes sense that the best way to address security threats in the cloud is with a cloud-native security solution. These solutions are built in the cloud with the capabilities to handle today's varied architectures.

How's the technology witnessing adoption In India

India's public cloud market is among the largest in the Asia Pacific (APAC) region behind only Australia and Japan, according to new analysis from Boston Consulting Group (BCG). By 2023, the consulting firm expects the public cloud market in India to reach the US$8 billion mark from the current US$2.6 billion market @ CAGR of 25%. The global forecast according to Gartner is US$331.2B @ CAGR of 28.5% by 2022.

Key drivers for adoption

The reason behind this position of global dominance is the size of the population and consequently the cloud market in India, which gives it's the edge over other digitalizing markets. Previous analysis from BCG has predicted that the country will have as many as 850 million online users by 2025.

By 2023, BCG predicts that the public cloud market could have contributed as much as US$102 billion to the Indian economy in direct and indirect value. Growth in the market is also likely to create employment, enumerated by BCG at approximately 980,000 jobs over the same period[2].

Public and manufacturing sectors have low adoption rates and the sectors with high adoption rates are financial services, retail and consumers services, media and gaming and digital natives.

Industry reports around the world believe that cloud technology is a critical enabler of the Industrial Revolution 4.0. As the new industrial revolution is ignited, cloud computing is effectively supporting the developments of the IoT, automation and robotics. It is very evident that the cloud security software market is poised for strong growth in the coming years. Organizations today are dependent to a large extent on cloud-based services for a majority of the operations and managing various data. On the other hand, cyberattacks, vulnerabilities and breaches are also increasing, leading to security concerns

[2] BCG Report, Ascent to the cloud

1

about the safety of data on the cloud. With employees remotely working, there is an increase in employee mobility with the adoption of Bring your own device (BYOD) and IoT services. These aspects have brought about a growing demand for cloud computing. This has led to the adoption of cloud-based security solutions, thereby, spurring the growth of cloud security market globally.

According to one of the reports published by Orbis Research recently, the cloud security software market was valued at US$28.1 billion in 2018, is expected to reach US$35.6 billion by 2024, at 4.98% CAGR during the forecast period 2019-2024[3].

There is flexibility in building cloud solutions for specific requirements of businesses and they defend a set of authentication regulation of devices and users. Consumers' privacy and critical data storage are also maintained. Cloud security is becoming more imperative and complex than before, leading to exponential growth in the cloud security software market.

The needs of the organization for application and data storage are getting more complicated. So is the IT infrastructure, as the public cloud cannot be leveraged for all applications due to privacy concerns.

A hybrid cloud environment that connects a mix of public cloud, private cloud and on-premises IT infrastructure, is in more demand as it suits the different needs of an organization. Organizations have the flexibility to migrate to cloud technology as and when they wish to.

Multi-cloud strategies are expected to play a key role in the near future. These enable users to leverage any cloud solution (private, public or hybrid) depending on their technical requirements.

[2]BCG Report, Ascent to the cloud

Cyber threats and challenges

Why cloud security is different

Cloud-native security solutions, built specifically to protect cloud resources, excel where traditional on-premises security solutions struggle. Here’s a breakdown of how cloud and traditional security solutions address major challenges:

Challenge	Traditional security	Cloud security
Visibility	Monitoring of on-premises resources and limited monitoring of cloud resources.	Monitoring of both on-premises and cloud resources. On-premises resources across different locations can be monitored without having additional security appliances at each site.
Deployment	Security appliances must be procured, shipped to each site, installed and configured. Given the new infrastructure and initial configuration, deployment issues are common. Gartner says that over 50% of SIEM deployments fail.	SaaS model eliminates the need to deploy hardware or software. Saves time on change management, facility, provisioning, etc. Runs on an established platform, so deployment issues are rare.
Time to value	Typical project lifecycle–procure, ship, install, configure, tune–causes slow time to value. Long cycles for updating, managing, and running the use cases, etc. Most deployments run more than nine months and you cannot usually see value in the first year.	Rapid deployment, built-in and updated content, updated use cases, simplified user experience gives you to get started on security in just few hours or days.
Maintenance	Handled by in-house IT and security teams. This is a big point of failure. We see more customers looking for cloud solutions after they go through a maintenance cycle and stop seeing value.	Handled by cloud service provider (CSP). The vendors usually update the platform every day and update features and bugs more frequently. It is typical for cloud vendors to have 12 releases a year where software/ appliances will be updates once a year.
Total cost of ownership and ROI	▶ Capex based ▶ Big budgetary investments ▶ Long planning and deployment cycles ▶ Multiple groups from security, IT, facilities, ops, DevOps, to LOB and apps are all involved ▶ Licensing cost is only 9% of the TCO. HW/SW/facilities and other hidden costs are involved ▶ Tough to predict the pricing for the next quarter/ year	▶ Opex based ▶ Consumption model ▶ Subscription based ▶ No long term contracts ▶ Easy to replace vendors if there is no fit ▶ Low risk solutions ▶ Payback is typically six to nine months ▶ Subscription cost covers almost 70% of the TCO
Updates and patches	▶ Requires periodic maintenance windows and planned outages ▶ Unpatched systems are a big threat for security	▶ Cloud vendors take care of updates and patches through the shared responsibility model ▶ Low risk of vulnerabilities for unpatched systems
Capacity planning and elasticity	▶ HW, SW and licensing needs to be planned for over capacity for occasional bursts or peaks ▶ Your TCO is designed on seasonal peaks ▶ Extreme bursts lock you out of tools when you need the most	▶ No planning needed for capacity ▶ Elastic scaling takes care of unplanned capacity planning ▶ Seasonality, peaks and bursts are handled effortlessly

Traditional on-premises security provides analysis and insight using a Security Information and Event Management (SIEM) system.

Skills a CISO needs to focus on

With continued growth in adoption of cloud in enterprises the information part, or the I in CISO, is going away from a nomenclature perspective. Where security was once largely focused on information security, today it includes a broader category of responsibilities including and applications running in the cloud.

The cloud has facilitated software development which means there are entire businesses today that are built solely on applications in the cloud. This means the crown jewels of the business are also in the cloud and so the hygiene piece we didn't get right in on-prem has carried over to the cloud and gotten worse.

As a result, the role of a modern CISO is in many ways about adversary hunting. More importantly, it requires defining that in a way that is meaningful to the organization – and partnering with developers to implement controls and best practices to implement it. Partnering is the operative word because development doesn't report to the CISO, yet in a cloud environment, it's critical to overall security. In many ways, this is a cultural shift in the role that has caused some researchers to conclude an essential skill of high performing CISOs is to learn to lead without authority.

The skills that separate one CISO from another, center on the ability to both to explain the complexities of dynamic adversaries to both a technical audience, such as DevOps and to a business audience, like the C-Suite or the board of directors. In addition, information must be articulated in a manner that gives the organization confidence in the security program.

The challenge is that talking with and persuading developers is an entirely different skill set than speaking to and influencing a board of directors. This requires cross-functional experience and the combination of these talents is so rare.

CISO must continuously adapt to the constantly changing cloud environment. The cloud computing characteristics that are driving the move to the cloud are exactly the reasons a new security model is needed. Cloud environments are constantly changing by design.

According to the National Institute of Standards and Technology (NIST) definition, cloud computing uses computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This has manifested itself today in the form of containers, microservices, and serverless computing.

These newer technologies provide the hyper scalability and elasticity of cloud computing. Services are spun up and taken down to meet demand and transient events. Traditional security cannot react to these changes in an effective way.

To be secure, the cloud needs cloud-native security solutions that meet these criteria:

- Visibility into containers, microservices and serverless
- Ability to monitor and analyze transient and elastic workload data
- A holistic view of the entire threat surface
- True software-as-a-service (SaaS) security solution

5G

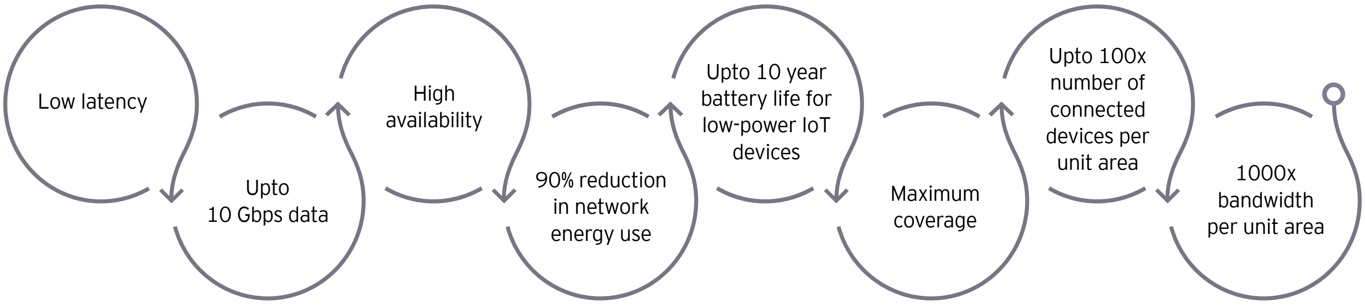
2

5G

Telecommunications services will play a pivotal role in the digital economy for decades to come. The term 5G has become a buzz word in today's world, however, it has not been many years since it was introduced and used for the first time.

5G is the next generation of wireless networks, building upon the existing 4G Long-Term Evolution (LTE) infrastructure and improving the bandwidth, capacity and reliability of wireless broadband services.

Features of 5G technology



Low latency

Upto 10 Gbps data

High availability

90% reduction in network energy use

Upto 10 year battery life for low-power IoT devices

Maximum coverage

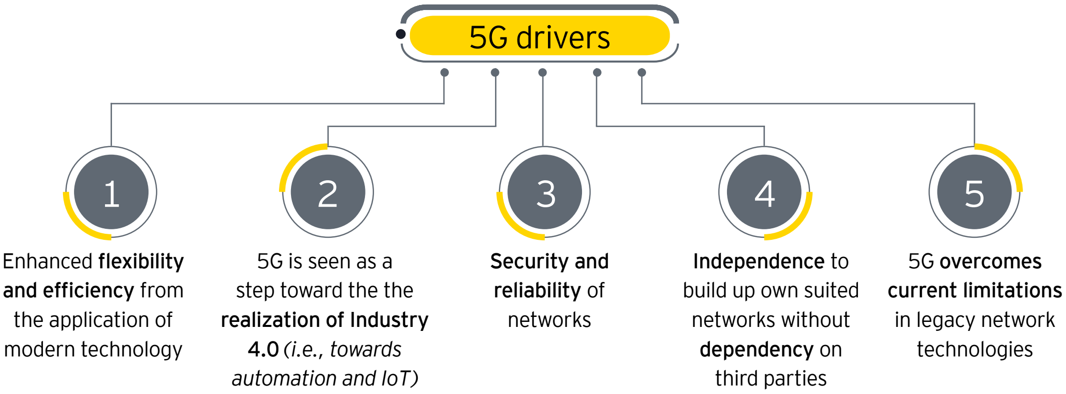
Upto 100x number of connected devices per unit area

1000x bandwidth per unit area

With enhanced features and capabilities 5G will open new business opportunities which were not possible in the 4G era. Opportunities centered around high-speed mobile broadband, massive IoT enabled infrastructure, smart transportations, robotic surgeries and augmented reality are now within reach.

Key drivers for adoption

5G is more than an evolution of mobile broadband. It will be a key enabler of the future digital world, the next generation of ubiquitous ultra-high broadband infrastructure that will support the transformation of processes in all economic sectors and the growing consumer market demand.



5G drivers

1 Enhanced **flexibility and efficiency** from the application of modern technology

2 5G is seen as a step toward the the **realization of Industry 4.0** *(i.e., towards automation and IoT)*

3 **Security and reliability** of networks

4 **Independence** to build up own suited networks without **dependency** on third parties

5 5G **overcomes current limitations** in legacy network technologies

With respect to security standpoint, 5G will have a wider security threat landscape due the IT-driven architecture, amalgamation of newer nonstandard technologies and non-standard radio access methods. Considering these challenges standardization of 5G becomes very important for a safer world.

2

1 **Traffic embezzlement**

The use of multiple layer of virtualization such as SDN and NFV opens new avenues for attackers. The software used in SDN and NFV will introduce security threats such as data forging, API abuse, controller and management exploitation

2 **Weak slice isolation**

A weak slice isolation or connection could threaten to bring down the 5G network by compromising sensitive data contained in a slice as well as exposing other slices to attacks and the risk is higher due to distribution of isolation over underlying security domains which could increase complexity if improperly managed.

3 **Cyber threats and challenges**

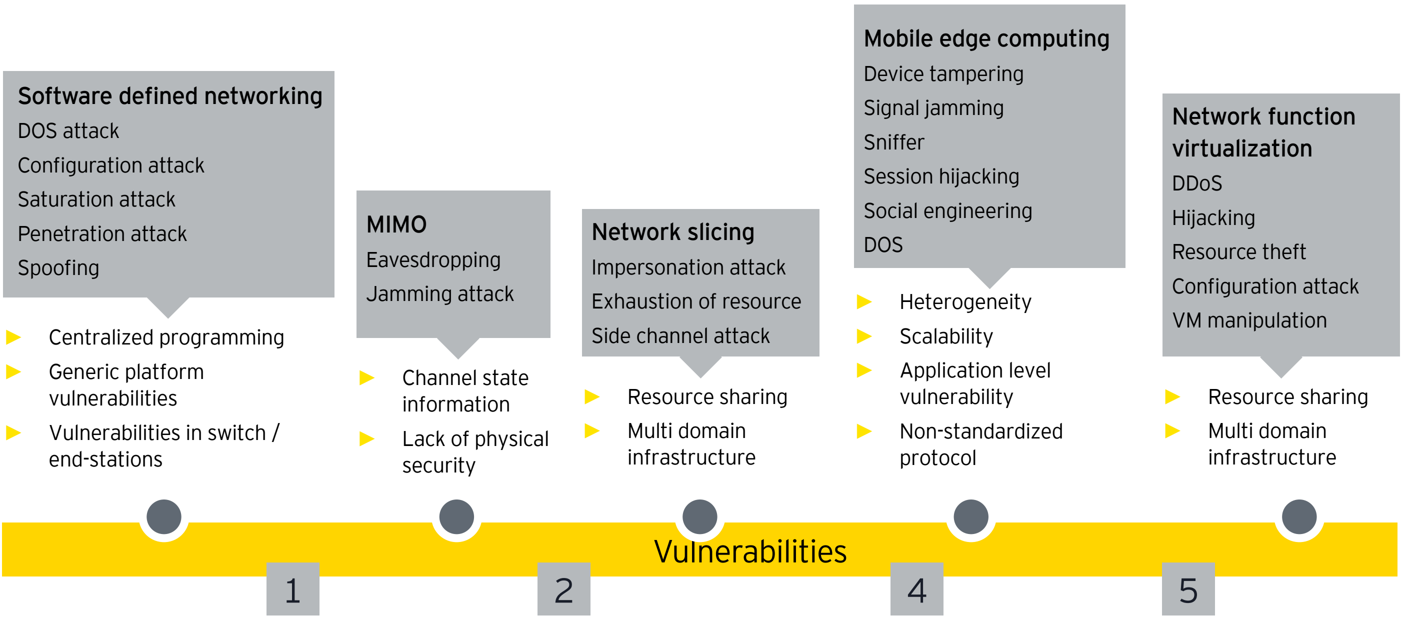
A cloud-native 5G architecture may spawn an entirely new ecosystem of technological and enterprise innovations which will support a wide range of new applications in the consumer and business segments including markets such as manufacturing, energy, healthcare and automobiles enabling which will further open new gates for information security breaches. Key skills need to be considered by CISO of an organization considering 5G.

4 **Unauthorized access to assets**

The 5G network will be heterogeneous combination of many network slices. Each network slice will have their own set of access controls that will vary from slice to slice. Multiple or nonstandard access control level will make network more vulnerable and may lead to risks like identity theft.

5 **Trust management**

Trust models are primarily developed to define various stakeholder's responsibilities, establish security policies and analyze the security of a telecommunication system. The challenge in 5G networks is due to the diversity of stakeholders due to virtualization technology increases the complexity of the trust model.



Software defined networking
DOS attack
Configuration attack
Saturation attack
Penetration attack
Spoofing

- Centralized programming
- Generic platform vulnerabilities
- Vulnerabilities in switch / end-stations

MIMO
Eavesdropping
Jamming attack

- Channel state information
- Lack of physical security

Network slicing
Impersonation attack
Exhaustion of resource
Side channel attack

- Resource sharing
- Multi domain infrastructure

Mobile edge computing
Device tampering
Signal jamming
Sniffer
Session hijacking
Social engineering
DOS

- Heterogeneity
- Scalability
- Application level vulnerability
- Non-standardized protocol

Network function virtualization
DDoS
Hijacking
Resource theft
Configuration attack
VM manipulation

- Resource sharing
- Multi domain infrastructure

Skills a CISO needs to focus on

Machine learning and Artificial Intelligence

ML and AI can be used in enhancing the security of 5G networks and preventing attacks and frauds by recognizing user patterns through automated algorithms and tagging certain events to prevent similar attacks in future

SDN and cloud security

Using software defined network (SDN) and cloud security with 5G is essential as it goes beyond the traditional N/w perimeter. A good way to segregate traffic and ensure rules are always up-to-date without the need for patching and upgrading

Internet of Things (IoT)

Rolling out of 5G will cause the number of IoT devices to increase exponentially, which will lead to the size of potential botnets being quite incredible and therefore require more focus on security in the IoT domain

Privacy

5G networks will allow us to connect more devices to the network and encourage us to capture and share more of our personal data. Also, to address growing concern and privacy, legislation in the 5G system will include subscribers' privacy by design.

Identity access management

The 5G ecosystem would need more flexible and open identity management infrastructure, which should have the scope for various alternatives as there would be an immense number of handheld devices therefore it is important to find ways on how to handle these devices

3

OT

OT

Operational technology (OT) is the hardware and software that detects or causes a change through direct monitoring and/or control of physical devices, processes and events in the enterprise. OT is common in Industrial Control Systems (ICS). For many years, ICS relied upon proprietary protocols and software and were managed manually with no connection to the outside world. For this reason, they were an insignificant target for hackers as there was no networked interface to attack and nothing to gain or destroy. Today, OT may be used to control power stations or public transportation. As this technology advances and converges with IT, the need for OT security grows exponentially.

Few factors that are elevating the risk landscape of OT/IoT environments are:

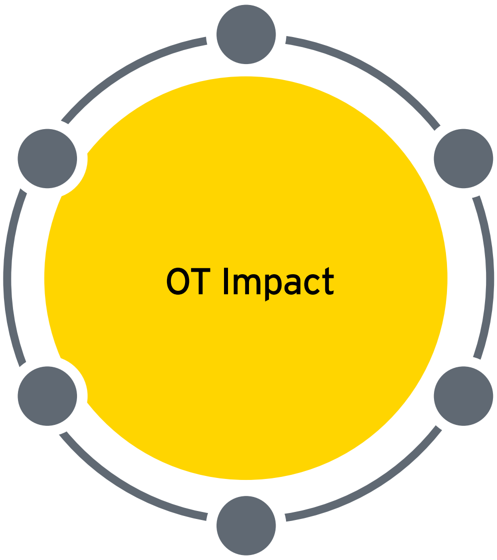
- Business requirement to process information from control systems to business users is increasing, thus converging OT and IT. However, IT and OT are still owned by different teams increasing the risk of vulnerabilities.
- Operational technology is becoming increasingly accessible, with threat vectors targeting base-level assets. Worms and viruses are being created specifically to damage control systems and thus increasing cyberattacks on OT.
- Many organizations are still running legacy systems with limited security capabilities.
- With the introduction of new technologies there is increased level of data exchange increasing the risk posture of OT systems and IoT devices.

Software defined networking

While the cost and efficiency benefits of OT remote support services are clear, organizations cannot afford to delay getting to grips with their information security implications

New trends in the workplace

These risks stem from both internal and external threats, including poorly implemented personal device strategy, mismanagement of the device itself, external manipulation of software vulnerabilities and the deployment of poorly tested, unreliable applications in the plant environment



Reputational damage

With the speed and complexity of the threat landscape changing on a daily basis, all too often businesses are being left behind, sometimes in the wake of operational reputational damage. As national critical infrastructures the reputation may affect the public and foreign trust in the country

The Internet of Things

As increased interest in setting security standards for IoT escalates, it should be up to the companies themselves to continue to build security through communication and interoperability

ICS regulations and equipment damage

Organizations need to treat OT security as both a compliance, operational and business risk issue to reduce regulatory sanctions and impacts

Safety

Cyber space is an increasingly attractive hunting ground for criminals, activists and terrorists. OT cyber attacks can cause disruption or even compromise the life and safety of the personnel

3

Key drivers for adoption

1

Remote support and maintenance

While the cost and efficiency benefits of OT remote support services are clear, organization need to expedite to tackle OT security challenges and attacks implication

2

Reputational damage

With the speed and complexity of the threat landscape changing daily, all too often businesses are being left behind, sometimes in the wake of operational reputational damage. As national critical infrastructures the reputation may affect the public and foreign trust in the country.

3

ICS regulations and equipment damage

Organizations need to treat OT security as both a compliance, operational and business risk issue to reduce regulatory sanctions and impacts.

4

Safety

Cyberspace is an increasingly attractive hunting ground for criminals, activists and terrorists OT cyber-attacks can cause disruption or even compromise the life and safety of the personnel.

5

Internet of Things

As increased interest in setting security standards for the internet of things (IoT) escalates, it should be up to the companies themselves to continue to build security through communication and interoperability.

6

Hybrid and multi-cloud

These risks stem from both internal and external threats, including poorly implemented personal device strategy, mismanagement of the device itself, external manipulation of software vulnerabilities and the deployment of poorly tested, unreliable applications in the plant environment.

Cyber threats and challenges

Cyber threats are increasing in number and sophistication. The motives behind attacks are many, including ideology, financial gain and espionage. A cyberattack on an OT environment can have catastrophic consequences like prolonged outages of critical OT devices, damage to equipment and financial losses.

Common attack vendors

- Web application attacks
- Client-side attacks
- Network attacks
- Malware and APTs (Advanced Persistent Threats)
- DOS/DDOS
- Social engineering/spear phishing
- Brute force attacks
- MITM (Man- in-the-Middle) and interception attacks
- Routing attacks
- Supply chain contamination attacks
- DNS attacks
- Evading/bypassing perimeter protection devices etc.

Impact of OT Cyber Attack

- Plant Sabotage
- Shutdown of plants, equipment
- Damage to equipment
- Production Disruption
- Compliance violation
- Safety violation

Looming Global Threat Environment – Recent Survey Results

2020 global ICS and IIoT risk analysis survey by CyberX showcases that[4]

21% of industrial sites have at least one direct connection to the public internet

71% of sites have obsolete Windows systems such as Windows XP and Windows 7

64% of sites have plain-text passwords traversing their ICS networks

66% of sites aren't running anti-virus protections that update signatures automatically

54% of industrial sites have at least one remotely accessible device

22% of sites exhibited indicators of threats

1 IoT devices experience an average of 5,200 attacks per month.

2 Routers and connected cameras are the most infected devices and accounted for 75% and 15% of the attacks respectively.

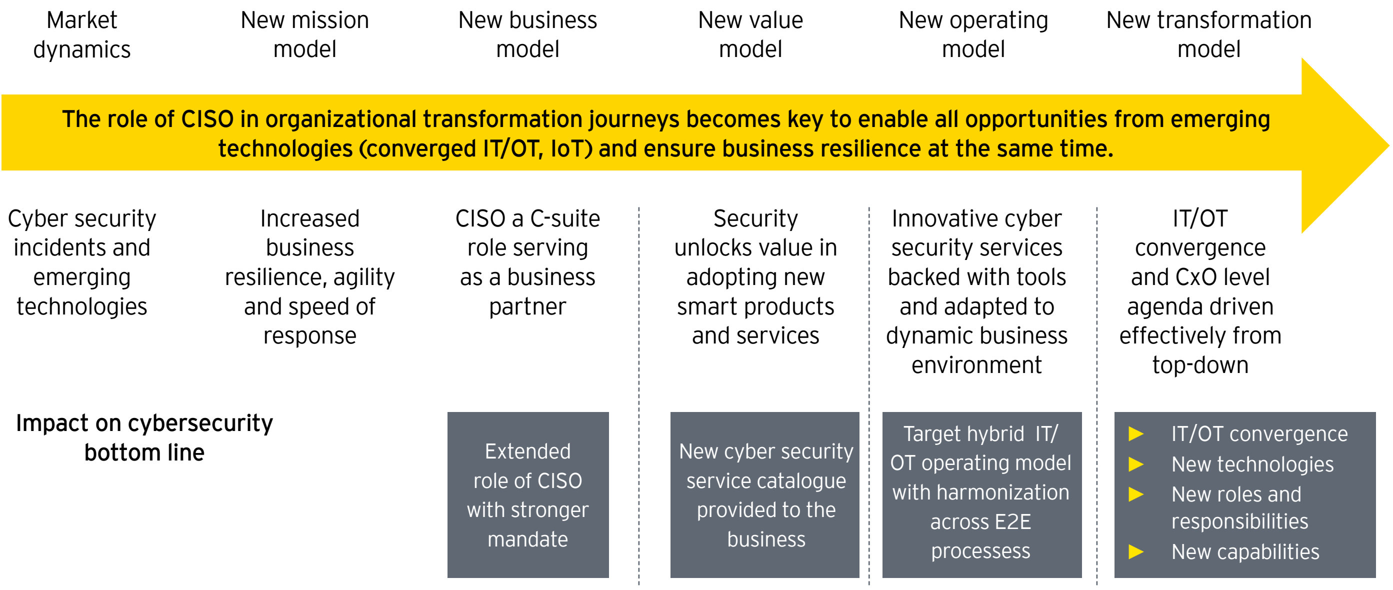
3 The notorious Mirai distributed denial of service (DDoS) worm remained an active threat and, with 16% of the attacks, was the third most common IoT threat in 2018.

4 VPN Filter was the first widespread persistent IoT threat, with its ability to survive a reboot making it very difficult to remove[5].

[5] 2019 global ICS and IIoT risk analysis survey by Cybex

Skills a CISO needs to focus on

The role of OT cybersecurity and CISO in modern organizational transformation journeys.



The role of CISO in organizational transformation journeys becomes key to enable all opportunities from emerging technologies (converged IT/OT, IoT) and ensure business resilience at the same time.

Market dynamics	New mission model	New business model	New value model	New operating model	New transformation model
Cyber security incidents and emerging technologies	Increased business resilience, agility and speed of response	CISO a C-suite role serving as a business partner	Security unlocks value in adopting new smart products and services	Innovative cyber security services backed with tools and adapted to dynamic business environment	IT/OT convergence and CxO level agenda driven effectively from top-down
Impact on cybersecurity bottom line		Extended role of CISO with stronger mandate	New cyber security service catalogue provided to the business	Target hybrid IT/ OT operating model with harmonization across E2E processess	► IT/OT convergence ► New technologies ► New roles and responsibilities ► New capabilities

The world is changing and so is the role of OT cybersecurity and CISO in the organization. An effectively converged IT/OT and CxO-driven agenda can form the heart of an organization's operational defense against advanced OT cyberattacks.

The role of CISO in the organization transformation journeys is the key enabler in creating more resilient OT networks through the effective use of skilled resources and suitable technology.

Business leaders should focus on harmonizing IT-OT operating model across E2E processes. Innovative cyber security services backed with tools can help build a secure and reliable defense mechanism against all types of IT/ OT cyberattacks.

Leaders should also focus on organization wide information security awareness and enforce strict implementation of information security policies, including the integration of defense in depth techniques around IT and OT networks to combat any vulnerabilities in the system.

Threats continue to evolve and your organization must too. It is important that organizations not only maintain traditional security controls but continue to evolve their ability to rapidly detect and respond to threats in the IT/ OT environment. It is critical that OT security initiatives are initiated with the correct balance between preventive, detective and reactive controls to help build resilient OT networks.

Data privacy

4

Data privacy

In today's digital age, a primary point of concern for the individuals is breach of their privacy. Internet penetration has grown tremendously in the last few years thanks to the growth of startups, e-commerce companies and technology offerings across industries. This transformation created the need of a strong regulation protecting personal data in the current era of technological revolution.

The formulation of GDPR in April 2016 also served as an awakening call to other regulators, creating a domino effect. Several other countries have recognized the need of a comprehensive and robust regulation to protect personal data and introduced their own data protection laws.

India has also followed suit with its draft Personal Data Protection Bill. India is a key player in the global technology ecosystem and has therefore uniquely positioned itself to establish its own practices and procedures for ensuring privacy and protection of personal data. As Indian businesses move towards significantly data-driven models, it is imperative for all stakeholders (government, independent regulatory bodies, organizations, and customers) to adopt a coordinated plan of action to enforce the obligations and requirements of Personal Data Protection Bill.

Data privacy in India

In today's digital age, a primary point of concern for the individuals is breach of their privacy. India has recognized this concern, however, through its Draft Personal Data Protection Bill (draft Bill). The draft Bill regulates the processing of personal data of individuals (data principals) by government and private entities (data fiduciaries), established in India as well as outside India (extra-territorial applicability). It specifies the conditions under which the personal data of individuals will be collected and how organizations can process the data collected by them.

India is inching towards becoming a digital economy and adoption of privacy practices

Currently, India ranks second in terms of the number of internet users in the world with over 560 million active users, which is estimated to shoot up to 730 million by 2020[6].

The Government of India is aiming to enhance the digital economy through its Digital India initiatives and e-governance projects. All such developments correspond to a humungous increase in user data, which is used to analyze user behavior for enabling various services.

Further, emerging technologies such as artificial intelligence, machine learning, Internet of Things and the cloud have made things possible which were a distant dream few years ago. Such services utilize sophisticated technology and inevitably requires large amount of user data.

These developments are serving as a cornerstone in the digital economy where data has been termed the new oil which, is no longer bound by physical boundaries or geographical restrictions.

Further, as organizations are understanding the importance of data privacy and security, technology adoption has also increased.

The adoption is focused on enhancement of the security and privacy posture through initiatives such as differential privacy which allows companies to collect user data in a format that allows identifying patterns of consumer behavior without violating their privacy. Using disruptive technology such as blockchains, organizations are storing the personal data of users on private blockchains and creating a new personal data economy. Organizations are using advanced data management tools to comply with the regulatory obligations of data minimization and data masking. Such tools offer comprehensive measures to discover, protect and manage sensitive data.

More connected devices

15.41 m in 2015

75.44 m in 2025

More users

330 m in 2015

730 m in 2025

Source: statista.com

[6] digitalindia.gov.in

4

India is charting its path to data privacy. Data privacy and the associated regulatory landscape is becoming the new building block of the Indian digital economy. With its own Personal Data Protection Bill, (PDPB), India is on way to becoming a truly digitally sovereign economy which would embrace technologies and regulations as they come.

Hence, there is an imperative need for data privacy to be inculcated in the DNA and culture of the organizations so that Right to Privacy can be realized in its true sense.

Key drivers for adoption

1 **Digital disruption**

With the Digital India rollout, push on digital payments and an exceptional number of platforms and services processing personal data of individuals, a stronger data protection regime is required to nurture trust in the data ecosystem.

2 **Increasing breaches**

Data breaches are at an all-time high, with new and evolving technologies being used to instigate as well as prevent cyber-attacks. With organizations facing a growing risk of being attacked, data privacy demands both defensive and offensive strategic solutions.

3 **Increasing regulations**

Indian organizations need to comply with the Personal Data Protection Bill-2019, when enforced. Additionally, Indian organizations need to manage global compliance since most data privacy regulations have extra-territorial application and non-compliance to the same can lead to hefty penalties and/or non-continuance of business

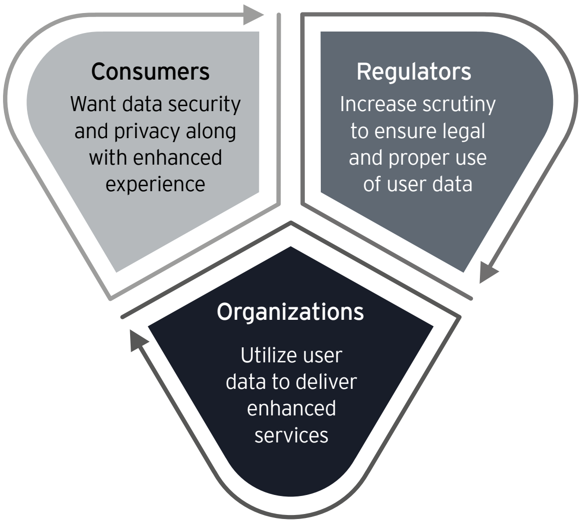
4 **Adequacy in cross border transfers**

India wants to strengthen its stance of data protection as it wants to gain its position as an adequate country for cross border transfers, for enhanced business growth.

5 **Competitive advantage**

Compliance with leading data privacy principles and standards is serving as a competitive edge for businesses.

Organizations will face a privacy paradox



Consumers
Want data security and privacy along with enhanced experience

Regulators
Increase scrutiny to ensure legal and proper use of user data

Organizations
Utilize user data to deliver enhanced services

Cyber threats and challenges

1

Privacy in digital landscape

With digital disruption and connected technologies, the risk of a data breach increases exponentially due to increased end points. Organizations need to assess their digital presence and ensure the security of personal data residing digitally.

2

Consent management

Organizations need to upskill their consent management abilities. While most organizations understand the concept of consent and have started obtaining it, the challenge is to manage, record and refresh it periodically.

3

Data management

Data forms the backbone of most organizations with personal and sensitive data continually passing through multiple IT applications. Identification and mapping of the widespread personal data involves effort- organizations will have to deploy tools to ensure adequate coverage.

4

Vendor management

The increased trend towards outsourcing development and support functions means that personal data of clients and employees is often accessed by external vendors, thus significantly increasing the data's net exposure.

5

Managing data principal rights

Right to be forgotten, erasure and portability add to the complexity due to wide distribution of data across different databases, backups, inter-company transfers, etc. For example, scouring a database for an individual's mention amongst billions of records/files and deleting them definitely poses performance challenges to databases, if it is not a new functionality altogether.

6

Privacy governance

Privacy is no longer exclusively situated within the legal realm but has evolved into a multi-disciplinary issue. Organizations are struggling to establish a comprehensive model to lead privacy transformation.

7

De-identification of data

Techniques like de-identification can be powerful tools in minimizing the impact of breaches and for companies to safely monetize their data. However, traditional techniques for de-identifying data (e.g., data swapping and suppression or stripping PII) provide little or no guarantee of privacy. Thus, using strong de-identification techniques is also posing a challenge to organizations.

8

Lack of automation

Manual processes and temporary work-arounds are prevalent in certain aspects of data management relevant to PDPB and other regulatory compliance- such as responding to data principal rights, data mapping and inventorization which is prone to human errors.

Skills a CISO needs to focus on

Since the threats to privacy and data protection are increasing, so is the risk of becoming a target of a data breach.

Cyber-crime can seriously damage brands, erode customer confidence, violate compliance mandates, and weaken the ability to generate revenue.

Thus, it is imperative for the CIO/CISO to incorporate privacy and data protection into the corporate DNA.

A CISO should have an in-depth understanding of privacy and data protection requirements and should be up-to-date with the Indian and global regulations, as applicable, for the organization.

Privacy is not just a technical issue but requires enhanced awareness and cultural change in the organization regarding data protection practices. A CISO must be able to drive such an organization level behavioral change.

Risk management is an integral part of privacy where the CISO needs to take an enterprise-wide view of the privacy risks and work in collaboration with IT, InfoSec, legal and the management.

In the era of technological developments, there is a pressing need to balance innovation and privacy where technology acts as an enabler for enhanced data protection. To truly succeed in the privacy revolution, CISOs need to embrace privacy and use it as a differentiator in the market so that the customers can entrust their personal information with the organization. To achieve that ideal state, CISOs need to tread their ways through implementation concerns, insufficient awareness and legislative ambiguities.

Recommendations

5

Recommendations

New technologies from cloud to 5G to OT promise to revolutionize India and enable digital transformation on a scale that seemed far-fetched a decade ago. Organizations need to understand that considering cyber risk and embedding cybersecurity from the start are imperative to success in the digital era. The focus should also be on how cybersecurity will support and enable enterprise growth with the aim of integrating and embedding security within business processes from the start.

1 Government would need to encourage development of stronger relationships between organizations across different sectors and government bodies for sharing Cyber intelligence and research information.

2 There should be enhanced focus to drive cyber-attack reporting to the Government/ CERT-In for all organizations registered in India.

3 Security-by-design should be a key principle as emerging technologies move centre stage. To achieve these goals, organizations will need an innovative cybersecurity strategy rather than responding in a piecemeal and reactive way.

4 The objective for all organizations should be to not only protect the enterprise with good cybersecurity hygiene and basic lines of defence, but also to optimize the response with more advanced tools and strategies.

5

5 Focus on emerging markets for business opportunities to stay relevant and profitable going into 2020 and beyond with adequate budgeting for cyber security.

6 A well planned audit program to evaluate the cybersecurity practices of the organization, internal control systems, and compliance with laws, regulations, and corporate policies concerning IT-related risks

7 The CISO's themselves as well as for their team need to upskill to be aware of newer technologies and their potential cyber risk.

As digital transformation proceeds, cybersecurity must be an enabling function rather than a block to innovation and change. Cybersecurity needs to be in the DNA of the organization; start by making it an integral part of technology adoption strategy. To ensure customer experience as an imperative it is essential to consider Cyber security as a collaborative effort. The first step begins with awareness of the changing technology and threat landscape. Cybersecurity needs to be mandated right at the start of technology transformations and followed throughout the entire lifecycle. CISOs need to build a strategy around the new methodologies needed for the next generation of cyber networks. As organizations mature in their experience of the sources and causes of the cyber risks in these areas, more action and initiatives from all dimensions may be expected. Global leading practices and innovative approaches must be looked at to solve security and privacy concerns.

About ASSOCHAM

The Knowledge Architect of Corporate India

Evolution of Value Creator

ASSOCHAM initiated its endeavour of value creation for Indian industry in 1920. Having in its fold more than 400 Chambers and Trade Associations, and serving more than 4,50,000 members from all over India. It has witnessed upswings as well as upheavals of Indian Economy, and contributed significantly by playing a catalytic role in shaping up the Trade, Commerce and Industrial environment of the country. Today, ASSOCHAM has emerged as the fountainhead of Knowledge for Indian industry, which is all set to redefine the dynamics of growth and development in the technology driven cyber age of 'Knowledge Based Economy'.

ASSOCHAM is seen as a forceful, proactive, forward looking institution equipping itself to meet the aspirations of corporate India in the new world of business.

ASSOCHAM is working towards creating a conducive environment of India business to compete globally. ASSOCHAM derives its strength from its Promoter Chambers and other Industry/ Regional Chambers/Associations spread all over the country.

Vision

Empower Indian enterprise by inculcating knowledge that will be the catalyst of growth in the barrierless technology driven global market and help them upscale, align and emerge as formidable player in respective business segments.

Mission

As a representative organ of Corporate India, ASSOCHAM articulates the genuine, legitimate needs and interests of its members. Its mission is to impact the policy and legislative environment so as to foster balanced economic, industrial and social development. We believe education, IT, BT, Health, Corporate Social responsibility and environment to be the critical success factors.

Members – Our Strength

ASSOCHAM represents the interests of more than 4,50,000 direct and indirect members across the country. Through its heterogeneous membership, ASSOCHAM combines the entrepreneurial spirit and business acumen of owners with management skills and expertise of professionals to set itself apart as a44 Chamber with a difference.

Currently, ASSOCHAM has more than 100 National Councils covering the entire gamut of economic activities in India. It has been especially acknowledged as a significant voice of Indian industry in the field of Aerospace and Defence, Auto and Auto Ancillaries, Arbitration & Legal Affairs, Corporate Social Responsibility, Environment & Safety, HR & Labour Affairs, Corporate Governance, Information Technology, Luxury and Lifestyle, Biotechnology, Telecom, Banking & Finance, Company Law, Corporate Finance, Economic and International Affairs, Tourism, MSMEs, Textiles, Civil Aviation, Infrastructure, Energy & Power, Education, Legal Reforms, Real Estate and Rural Development, Startups & Skill Development to Mention a few.

Insight into 'New Business Models'

ASSOCHAM has been a significant contributory factor in the emergence of new-age Indian Corporates, characterized by a new mindset and global ambition for dominating the international business. The Chamber has addressed itself to the key areas like India as Investment Destination, Achieving International Competitiveness, Promoting International Trade, Corporate Strategies for Enhancing Stakeholders Value, Government Policies in sustaining India's Development, Infrastructure Development for enhancing India's Competitiveness, Building Indian MNCs, Role of Financial Sector the Catalyst for India's Transformation.

ASSOCHAM derives its strengths from the following Promoter Chambers: Bombay Chamber of Commerce & Industry, Mumbai; Cochin Chambers of Commerce & Industry, Cochin: Indian Merchant's Chamber, Mumbai; The Madras Chamber of Commerce and Industry, Chennai; PHD Chamber of Commerce and Industry, New Delhi. Together, we can make a significant difference to the burden that our nationcarries and bring in a bright, new tomorrow for our nation.

ASSOCHAM Contact

Deepak Sood
Secretary General, ASSOCHAM

Mail: sg@assocham.com

The Associated Chambers of Commerce and Industry of India Corporate

Office: 5, Sardar Patel Marg, Chanakyapuri, New Delhi-110 021
Tel: 011-46550555 (Hunting Line) | Fax: 011-23017008, 23017009 | Website: www.assocham.orgham's Region

EY Contacts

Rohit Mathur
Risk Advisory Leader
Email: Rohit.Mathur@in.ey.com

Murali Rao
India Cyber Leader
Murali.Rao@in.ey.com

Vidur Gupta
Partner - Cyber Security
Email: Vidur.Gupta@in.ey.com

Burgess Cooper
Partner - Cyber Security
Email: Burgess.Cooper@in.ey.com

Jaspreet Singh
Partner - Cyber Security
Email: Jaspreet.Singh@in.ey.com

Kartik Shinde
Partner - Cyber Security
Email: Kartik.Shinde@in.ey.com

Mini Gupta
Partner - Cyber Security
Email: Mini.Gupta@in.ey.com

Prashant Choudhary
Partner - Cyber Security
Email: Prashant.Choudhary@in.ey.com

Tiffy Isaac
Partner - Cyber Security
Email: Tiffy.Isaac@in.ey.com

Sambit Sinha
Partner - Cyber Security
Email: Sambit.Sinha@in.ey.com

Binu Chacko
Partner - Cyber Security
Email: Binu.Chacko1@in.ey.com

Sameer Paradia
Partner - Cyber Security
Email: Sameer.Paradia@in.ey.com

Prashant Gupta
Partner - Cyber Security
Email: Prashant.Gupta2@in.ey.com

Contributors

Amit Mittal

Lalit Kalra

Aseem Mukhi

Supriya Uppal Kumar

Jyoti Saini

Aditya Sharma

Our offices

Ahmedabad

22nd Floor, B Wing, Privilon,
Ambli BRT Road, Behind Iskcon
Temple, Off SG Highway,
Ahmedabad - 380 015
Tel: + 91 79 6608 3800

Bengaluru

6th, 12th & 13th floor
"UB City", Canberra Block
No.24 Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 6727 5000

Ground Floor, 'A' wing
Divyasree Chambers
# 11, O'Shaughnessy Road
Langford Gardens
Bengaluru - 560 025
Tel: + 91 80 6727 5000

Chandigarh

1st Floor, SCO: 166-167
Sector 9-C, Madhya Marg
Chandigarh - 160 009
Tel: + 91 172 331 7800

Chennai

Tidel Park, 6th & 7th Floor
A Block, No.4, Rajiv Gandhi Salai
Taramani, Chennai - 600 113
Tel: + 91 44 6654 8100

Delhi NCR

Golf View Corporate Tower B
Sector 42, Sector Road
Gurgaon - 122 002
Tel: + 91 124 443 4000

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity, New Delhi - 110 037
Tel: + 91 11 4731 8000

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
NOIDA - 201 304
Gautam Budh Nagar, U.P.
Tel: + 91 120 671 7000

Hyderabad

THE SKYVIEW 10
18th Floor, "Zone A"
Survey No 83/1, Raidurgam
Hyderabad - 500032
Tel: + 91 40 6736 2000

Jamshedpur

1st Floor, Shantiniketan Building
Holding No. 1, SB Shop Area
Bistupur, Jamshedpur – 831 001
Tel: + 91 657 663 1000

Kochi

9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel: + 91 484 433 4000

Kolkata

22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400

Mumbai

14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400 028
Tel: + 91 22 6192 0000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai - 400 063
Tel: + 91 22 6192 0000

Pune

C-401, 4th floor
Panchshil Tech Park
Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 4912 6000

Ernst & Young LLP

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

EYIN2002-012
ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither Ernst & Young LLP nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

RG

ey.com/in

@EY_India EY EY India EY Careers India @ey_indiacareers

About ASSOCHAM

The Associated Chambers of Commerce and Industry of India (ASSOCHAM), India's premier apex chamber, initiated its endeavour of value creation for Indian industries in 1920. Having in its fold more than 400 chambers and trade associations and serving more than 4.5 lakh members from all over India, it has contributed significantly to the economy by playing a catalytic role in shaping up the trade, commerce and industrial environment of the country. It has significantly contributed in the emergence of new-age Indian corporates, characterised by a new mindset and global ambition for dominating the international business. Known as the fountain-head of knowledge for the Indian industries, ASSOCHAM has emerged as forceful, proactive, forward looking institution that is equipped to meet the aspirations of corporate India in the new world of business.

Ready to redefine the dynamics of growth and development in the technology driven cyber age, it aims empower Indian enterprises by inculcating knowledge that will prove to be the catalyst of growth in the technology driven global market. ASSOCHAM aims to help and guide businesses to upscale, align and emerge as formidable players in their respective business segments. Its mission is to impact the policy and legislative environment so as to foster balanced economic, industrial and social development.

ASSOCHAM is working towards creating a model business environment in India that is at par with the rest of the world and that of a developed economy. It derives its strength from its promoter chambers and other industry/regional chambers/associations spread all over the country.

ASSOCHAM Offices
The Associated Chambers of Commerce and Industry of India (ASSOCHAM) 5 Sardar Patel Marg, Chankyapuri,
New Delhi - 110021

Tel: 46550555 (Hunting Line)
Fax: 011-23017008/9
Website: www.assocham.org