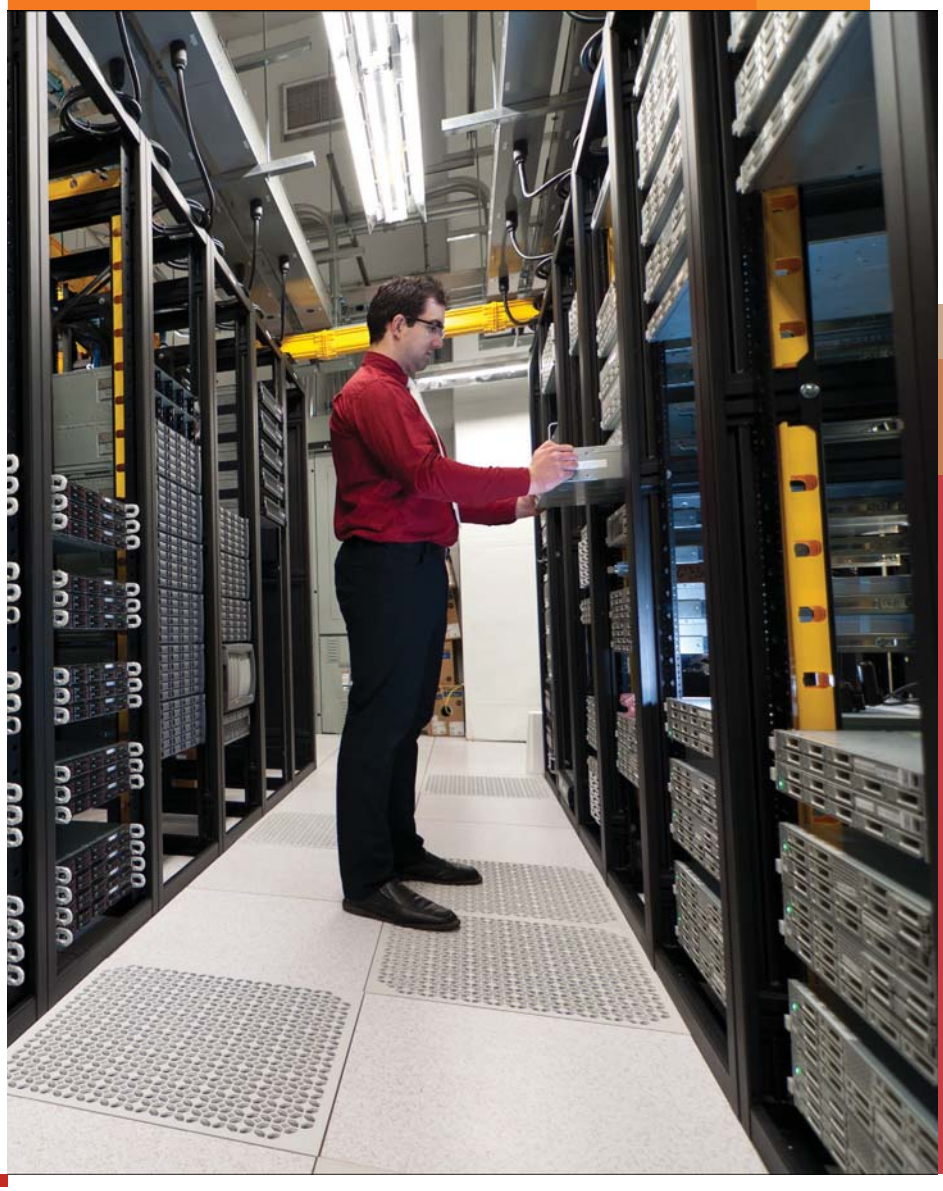
www.pwc.in

Protecting interconnected systems in the cyber era

ASSOCHAM
INDIA



pwc

Message from PwC

Sivarama Krishnan
Leader, Cyber Security
PwC India

The importance of cyber security in India has increased exponentially over the last few years, with an emphasis on Digital India and e-commerce and many government services now being delivered online. Cyber security has been identified as one of the key areas of development by the Honourable Prime Minister Narendra Modi. 'Can we secure the world from the bloodless war? I'm talking about cyber security. India must take the lead in cyber security through innovation. I dream of Digital India where cyber security becomes an integral part of national security,' he recently said.[1]

The threat of cyberattacks is increasingly coming from a broader range of individuals and entities. This new breed of hacker understands cyber vulnerabilities and how to exploit them. And they play by a new set of rules. The 'bare minimum' is ineffective against increasingly adept assaults. Businesses need to rethink their cyber security practices and focus on innovative technologies that can help reduce risks. Companies who have the right data, understand data and know how to take active steps in putting the information to good use will enjoy an advantage.

As a society, we all depend on operational technology for a wide range of critical industrial processes. Operational systems are increasingly subject to cyberattacks, as many are built around legacy technologies with weaker protocols that are inherently more vulnerable. The continued and regular sharing of cyber security intelligence and insights is essential to improving the resiliency of these systems and processes to emerging cyber risks.

While the nation focusses on growth, our work as technologists, strategists and captains of industry is clearly cut out. We need to focus on the basics that will help keep the growth story on course and ensure that organisations in India adopt the right cyber security stance.

Through this knowledge paper, we have tried to capture the best practices which are prevalent across the globe for the protection of interconnected systems and which can assist organisations in India in building strong defences against cyberthreats, thus fostering organisational growth in this digital age.

1 *PTI. (2015). Digital India: PM Modi says India can play a big role in cyber security globally. NDTV. Retrieved from http://www.ndtv.com/india-news/digital-india-pm-modi-says-india-can-play-a-big-role-in-cyber-security-globally-777319*

Message from ASSOCHAM

Shri Pratyush Kumar
Chairman, ASSOCHAM National Council on Cyber Security
Vice President, Boeing International
President, Boeing India

We are living in a volatile world. The increasing and widespread threat of terrorism across the world, the geopolitical situation in the South China Sea, Brexit, the state of transition in the Middle East, the attempted coup in Turkey—all these factors are adding to uncertainty and volatility in the world. Concurrently, we are being deeply impacted by the furious pace of technological evolution, especially the big data explosion, mobility and the cloud, the Internet of things, machine learning, and analytics. If these technologies are properly managed, we can use them to transform our society. On the other hand, an uncertain and volatile world also puts this very technology in the hands of bad actors who can operate from anywhere in the world and cause tremendous damage, given the growing linkages between cyberspace and physical systems.

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

This is why the 9th edition of ASSOCHAM's Annual Summit on Cyber & Network Security is very timely. We look forward to a productive discussion on bridging people, process, and technology, which will require us to deal with questions of technology, law and privacy. We have appropriately named it Cyber 3.0 and welcome participants from the industry, academia, governments, security establishments and civil society to put forward solution- and action-oriented recommendations.

Message from ASSOCHAM

Babu Lal Jain
Co-Chairman, ASSOCHAM
National Council on Cyber Security

I am pleased to announce that ASSOCHAM will be holding its 9th Annual Summit on Cyber & Network Security this year, with participation from the government, leading industry experts and other key stakeholders.

The Internet has facilitated the quick adoption of technology by businesses and enterprises, making critical online transactions easier and effective. Mobile banking, online shopping, online trading and social networking have changed the way we do business and interact with clients. This has expanded opportunities and helped business grow faster. However, cybercrime is seriously affecting this progress. Criminals looking to steal data or disrupt commerce are targeting businesses of all sizes—big, medium or small. In fact, no business is too small to be a target. Small businesses can lose big.

Most countries around the world are facing a shortage of professionals who have the expertise, training and motivation to deal with cybercriminals.

India is no exception. Most of the technologies and cyber security tools used in India are imported. We probably do not have all the requisite skills to inspect these for hidden malware, Trojans, backdoors or flaws. Our knowledge of these vulnerabilities and weaknesses is limited to what we acquire through publicly available sources and vendor communication. Serious efforts are needed to build skills in this very sophisticated area of technology to either develop such hi-tech equipment ourselves, or at least set up high-end cyber labs that are capable of critically inspecting them before they are deployed in critical infrastructure and critical industry sectors.

I am happy that both the government and industry are taking several steps to ensure that cyberspace is secure. Events like this will go a long way in realising the vision of Digital India in an interconnected world.

Message from ASSOCHAM

D S Rawat
Secretary General, ASSOCHAM

Today, cyberspace touches almost every part of our daily life—be it through broadband networks, wireless signals, local networks or the massive grids that power our nation.

The threat from cyberattacks and malware is not only apparent but also very worrisome. A single solution cannot counter such threats. A good combination of law, people, process and technology must be established and then an effort made to harmonise the laws of various countries keeping in mind common security standards.

ASSOCHAM lauds the efforts made by the Government of India under the leadership of Shri Narendra Modi, Hon'ble Prime Minister of India, to ensure a secure and resilient cyberspace for citizens, businesses, and the government.

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 cyber security threats.

ASSOCHAM is privileged to be a member of the Joint Working Group (JWG) on Cyber Security set up by the National Security Council Secretariat (NSCS), Government of India; a member of the Cyber Regulation Advisory Committee and a member of the Joint Working Group on Digital India—both of which have been set up by the Ministry of Communications and IT, Government of India.

ASSOCHAM is committed to creating more awareness about cyber-related issues and this background paper, jointly prepared by PwC and ASSOCHAM, is a step in that direction. We congratulate the team for their efforts.

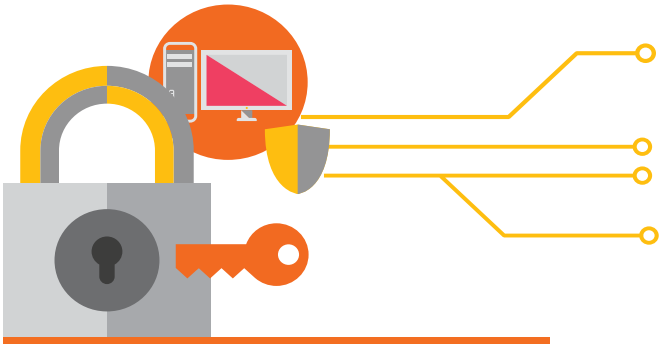
We convey our very best wishes for the success of ASSOCHAM'S 9th Annual Summit on Cyber & Network Security and hope that the summit will provide more insight into the emerging cyber-related challenges and appropriate solutions for further securing cyberspace.

1

Growth of interconnected systems

The world is moving into a space where everything and everyone is connected. This technological convergence has brought about numerous changes in our day-to-day lifestyles, redefined consumer relationships and enabled innovation for businesses. This convergence has grown stronger over time and technological dependence has increased to such a great extent that, today, we rely on some or the other form of technology for almost any aspect of our entire life. Today, business ecosystems have become an expanded universe of intelligent devices that are interconnected, indirectly or directly, via the Internet. This fusion of information technology (IT), operational technology (OT) and consumer technology (CT) has transformed business and society.

OT and CT systems have long been used in industrial and end-user products to monitor and control physical processes. Traditionally, these technologies have been air-gapped, in that they are segregated from the IT network. However, OT and CT systems are becoming increasingly interconnected and integrated with other IT systems. Economic challenges, resource constraints, business requirements and technology standardisation have made it impractical to continue completely segregating OT and CT networks from IT networks.

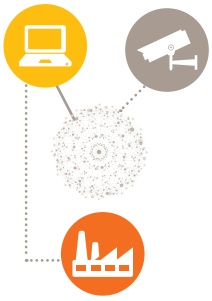


OT: Systems that control manufacturing processes

CT: End-user products and services such as home automation and sensor-enabled automobiles

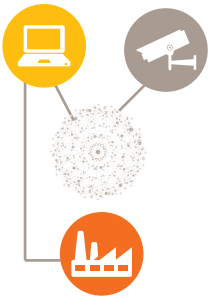
1980s

IT, OT and CT operated in different environments and on different platforms.



1990s

OT was networked to allow centralised operation. CT remained in a separate environment.



2000s

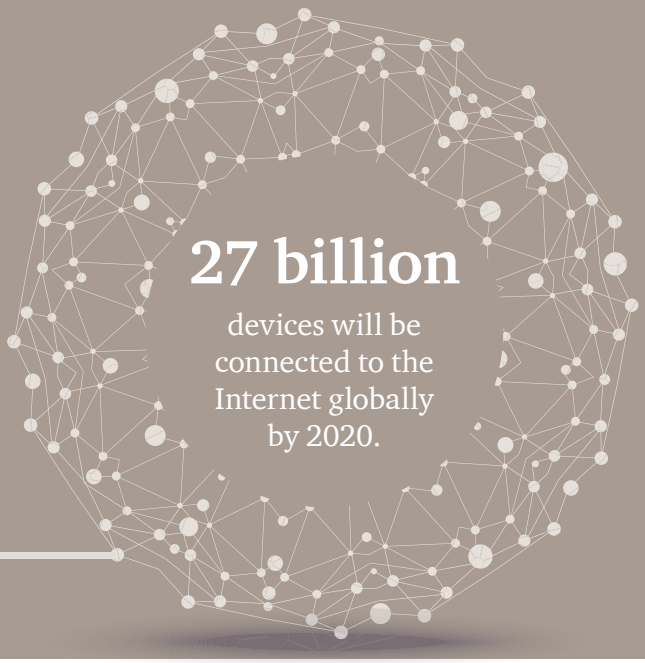
OT connected to IT using standardised IT channels. CT connected to IT through purpose-built channels.

2010+

The technology underlying IT becomes ubiquitous across OT and CT.

The number of Internet users in the world has increased threefold in the last 10 years.[2] During the same period, the number of Internet users increased nearly 15 times in India.[3] As per Gartner, the number of devices connected to the Internet will reach 27 billion globally in 2020, with a total revenue of around 300 billion USD. It is estimated that India will have an around 5–6% share of the global Internet of things (IoT) industry.[4]

Some examples of how interconnected systems have penetrated our lives and are providing convenience are given below: [5]



Smart distribution and transmission system

Utility companies across the globe are actively implementing smart distribution and transmission technology in order to secure efficiency, cost gains, and reduced system outages. Smart distribution and transmission systems use OT systems and other automation devices to increase response times to localised power outages and to gather grid performance data faster.

Intelligent transportation network

The transport system today has become highly automated and increasingly sophisticated technology is being used. An intelligent transportation network provides for various smart systems, such as intelligent traffic systems, autonomous vehicles and Positive Train Control (PTC).

- Autonomous vehicles: Automobiles contain dozens of computers that are often linked to each other and the Internet via wireless networks. Autonomous vehicles can steer, select, optimise speed, avoid obstacles, choose efficient routes, park, and warn passengers of any dangers, thereby enabling drivers to become passengers who are completely disengaged from the task of driving.
- Intelligent traffic system: Intelligent traffic systems have been set up in various cities of the world, enabling officials to monitor and streamline traffic conditions and manage traffic in cases of accidents and congestion.
- PTC: It is a system of automated control devices and remote sensors designed to stop or slow a train in order to prevent accidents. PTC is used to avert train-to-train collisions, unauthorised movement or derailments by utilising wired and wireless connections and automated acceleration and deceleration controls.

Home automation

Today, people can use a smartphone to adjust the room temperature at home while sitting in an office. A number of home automation devices have effortlessly blended into our lives thanks to IoT, making things easier and smarter and providing convenience.

Wearable devices in the e-health domain

A myriad of wearable devices have made their way into the market, ranging from fitness bands that monitor activity and sleep patterns to flexible patches that can detect body temperature, heart rate, hydration level and more. Through the Internet, physiological information can be shared in real time with the doctor for constant monitoring.

2 Internet Live Stats. Retrieved from http://www.internetlivestats.com/internet-users/#trend

3 Internet Live Stats. Retrieved from http://www.internetlivestats.com/internet-users/india/

4 Draft Policy on Internet of Things, Government of India. Retrieved from http://deity.gov.in/sites/upload_files/dit/files/Draft-IoT-Policy%20(1).pdf

5 The Future of Smart Cities: Cyber-Physical Infrastructure Risk, Department of Homeland Security. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf

2

Price of interconnectivity

The use of technology has enhanced productivity as well as efficiency. Factors such as the steady proliferation of data and growing interconnectivity are paving the way for new opportunities, while at the same time bringing to the forefront long-term challenges such as outages of critical services, environmental damage and even the loss of human life. Technology has led to new economic and social opportunities, but has also opened up more avenues for cyber attackers to cause disruption and carry out criminal activities. Change is happening at a fast pace, exposing those who are unprepared.

Cyberattacks around the world are occurring at a greater frequency and intensity. Not only individuals but also businesses and governments are being targeted. The profile and motivation of cyber attackers are 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.

Politically motivated or state-sponsored cyberattacks are carried out by members of extremist groups who gather information and commit sabotage. Cyberterrorism is the new weapon used by terrorists across the globe to inflict psychological and physical damage on their targets, in order to achieve their political gain or create fear within opponents or the public. They use cyberspace as a medium to spread propaganda, attack systems and steal money in order to fund their activities.

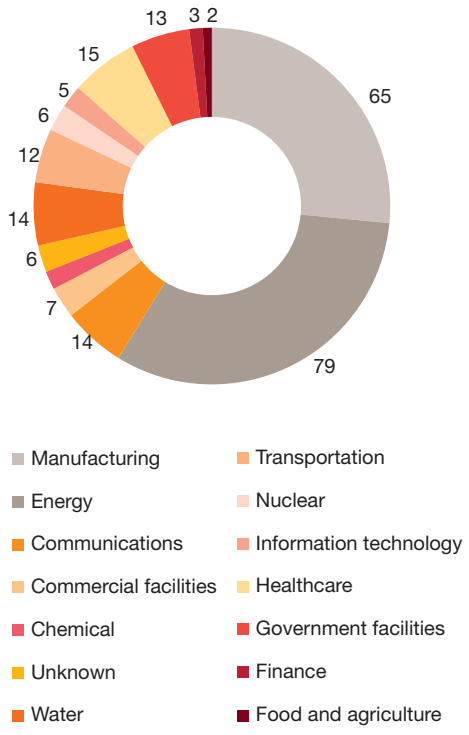
With every passing year, cyberattacks continue to escalate in frequency, severity as well as impact. In India, from 2011 to 2014, there has been a surge of approximately 300% in cybercrime cases registered under the Information Technology (IT) Act, 2000.[6] The Indian Computer Emergency Response Team (CERT-In) has also reported a surge in the number of incidents handled by it, with close to 50,000 security incidents in 2015.[7]

With an increase in the usage of information and OT and CT in critical infrastructure, overall effectiveness has increased. However, these elements have also become the target of choice for attackers since they recognise the impact of disrupting the routine way of life. Attackers can gain control of vital systems such as nuclear plants, railways, transportation or hospitals that can subsequently lead to dire consequences such as power failures, water pollution or floods, disruption of transportation systems and loss of life.

In the US alone, there has been an increase of nearly 50% in reported cyber incidents against its critical infrastructure from 2012 to 2015.[8]

> The motivation to commit a cybercrime now has gone far beyond financial to **political, economic and sociocultural** aspects.

No. of attacks in the US



Source: ICS-CERT Monitor (September 2014–February 2015)

6 National Crime Records Bureau (NCRB): Crime in India, PwC analysis

7 Indian Computer Emergency Response Team. Retrieved from www.cert-in.org.in

8 Meola, A. (2016). Cyberattacks against our critical infrastructure are likely to increase. Business Insider. Retrieved from http://www.businessinsider.com/cyber-attacks-against-our-critical-infrastructure-are-likely-to-increase-2016-5?IR=T

Over the past few years, virtually every industry sector across the globe has been confronted by some kind of cyberthreat. Some of the impactful incidents are as follows:

Hospital in the US remained shut for a week and had to pay a ransom in order to resume operations

A hospital in California had to shut down all its systems for a week as it was attacked by cybercriminals demanding a ransom of 40 bitcoins amounting to 17,000 USD. The hospital had to pay the amount in order to safeguard all patient records and restore the hijacked file.[9]

Hack attack causes 'massive damage' at German steel works

A blast furnace at a German steel mill caused massive damage following a cyberattack on the plant's network. It is believed that attackers used booby-trapped emails to steal logins that gave them access to the mill's control systems.[10]

Nuclear facility in Iran attacked by a computer worm destroying 1,000 nuclear centrifuges

In 2010, a nuclear facility in Natanz, Iran, was attacked by the Stuxnet computer worm. It is believed to have destroyed nearly 1,000 nuclear centrifuges, infecting about 60,000 computers in the process.[11]

Massive power outage in Ukraine due to malware within the networks of power companies

BlackEnergy malware was planted within the networks of multiple regional power companies in Ukraine and technical support phone lines of targeted firms were also flooded, which led to blackouts in different regions in Ukraine.[12]

Estonia faced a full-scale cyberwar

Estonia was subjected to cyberterrorism in which the attackers penetrated and brought down key government websites, rendering them redundant. A number of techniques such as ping floods and botnets were deployed for the penetration process.[13]

Mysterious pipeline blast in Turkey

Investigation into the Turkey pipeline blast pointed out that the blast did not trigger any distress signal, nor did cameras capture any combustion. However, later, it was found out to be a cyberattack where the hackers had disabled the alarm systems, cut off communications and super-pressurised the crude oil in the line.[14]

Email accounts breached at Pentagon's network

An incident of security snooping of Pentagon's unclassified emailing server was reported in August 2015, which led to a breach of the email accounts of around 4,000 military officials.[15]

Sabotage of traffic signals in Los Angeles

Two traffic signal engineers hacked into the systems and tweaked the timings of traffic signals at four critical intersections, causing havoc within the city.[16]

Critical services impacted in the US due to a computer worm

A computer worm named Slammer infected around 75,000 unpatched SQL servers, causing network outages and other consequences such as interference with elections, cancelled airline flights and ATM failures.[17]

---

9 Fox-Brewster, T. (2016). As ransomware crisis explodes, Hollywood Hospital coughs up $17,000 in Bitcoin. Forbes. Retrieved from http://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/#35a14ff475b0

10 BBC. (2014). Hack attack causes 'massive damage' at steel works. Retrieved from http://www.bbc.com/news/technology-30575104

11 Holloway, M. (2015). Stuxnet worm attack on Iranian nuclear facilities. Retrieved from http://large.stanford.edu/courses/2015/ph241/holloway1/

12 Kovacs, E. (2016). BlackEnergy malware used in Ukraine power grid attacks. SecurityWeek. Retrieved from http://www.securityweek.com/blackenergy-group-uses-destructive-plugin-ukraine-attacks

13 Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. Journal of Strategic Security. Retrieved from http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss

14 Robertson, J. & Riley, M. (2014). Mysterious '08 Turkey pipeline blast opened new Cyberwar. Bloomberg. Retrieved from http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

15 Harress, C. (2015). Pentagon hacked by Russia: 4,000 military and civilian records taken from joint chiefs of staff email system. International Business Times. Retrieved from http://www.ibtimes.com/pentagon-hacked-russia-4000-military-civilian-records-taken-joint-chiefs-staff-email-2042716

16 Pool, B. (2007). 2 accused of sabotaging traffic lights. Los Angeles Times. Retrieved from http://articles.latimes.com/2007/jan/06/local/me-trafficlights6

17 Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S., & Weaver, N. (2003). The spread of the Sapphire/Slammer worm. CAIDA. Retrieved from https://www.caida.org/publications/papers/2003/sapphire/sapphire.html


Login

3

Key cyber security challenges in interconnected systems

Business leaders today view security as a crucial part of their overall business strategy and are better positioned to balance the technologies, processes and resources required in order to combat myriad cyberattacks. However, the focus and spending on IT systems need to be complemented with similar efforts in the OT and CT systems. Currently, such initiatives are not taking place, thereby leading to a rise in attacks by cybercriminals. Based on our experience, some of the cyber security gaps in OT and CT are as follows:

Security governance: The ownership to secure OT and CT infrastructure is not clearly defined within organisations. The chief information security officer (CISO) is responsible for securing IT networks, while OT and CT systems are managed in isolation. Hence, there is no clear accountability defined for the security of OT and CT networks.

Basic security hygiene: Basic security hygiene for OT and CT networks is not maintained or given the same importance as that for IT systems. Some of the basic issues plaguing the systems include, but are not limited to, the following:

- Missing security updates
- Poor password practices
- Insecure encryption and authentication
- Lack of segregation within networks

Stakeholder awareness: Stakeholders, including third-party vendors, who are responsible for managing the networks and infrastructure have limited understanding with respect to security risks and vulnerabilities associated with OT and CT systems.

Security monitoring: While IT systems are monitored heavily for security purposes, monitoring of OT and CT systems is limited to process efficiency and performance. Hence, logs and events are not collected and correlated.

Incident response: Specific crisis management or incident response for OT and CT systems is different from that for traditional IT systems. Security plans specific to OT and CT are missing, thus increasing the potential impact of the incident.

By identifying cyber security flaws and issues, decision makers will be better placed to implement appropriate security controls, design additional secure architectures, monitor targeted attacks and maintain effective cyber resilience for their IT, OT and CT networks.

4

Gearing up to secure the world's interconnected systems

Governments and international bodies have realised the increasing threats to interconnected critical infrastructures and have taken serious steps to define and strengthen the cyber security of their respective systems.

US

The Department of Homeland has identified 16 critical infrastructure sectors, namely water and wastewater systems; the commercial facilities sector; transportation systems; nuclear reactors, materials, and waste; information technology; healthcare and public health; government facilities; the food and agriculture sector; financial services; the energy sector; emergency services; defence industrial base; dams; critical manufacturing; the communications sector; and the chemical sector. The assets and systems of critical infrastructure are considered so important that any harm to these may have an adverse impact on the country's security, economy and public health. Sector-specific plans have been defined for each of the critical infrastructure sectors. Some of the other important measures are as follows:[18]

National Infrastructure Protection Plan (NIPP 2013 – Partnering for Critical Infrastructure security and Resilience): It outlines the plan for collaboration among the government and private sector participants to manage risks and achieve cyber resilience.[19]

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community, and coordinating efforts among the Federal, state, local, and tribal governments as well as control systems owners, operators, and vendors.[20]

Protected Critical Infrastructure Information (PCII) Program: This enhances voluntary information sharing between infrastructure owners and operators as well as the government. PCII is used to analyse and secure critical infrastructure, identify vulnerabilities, develop risk assessments and enhance recovery measures.[21]

Canada

Canada's national critical infrastructure comprises 10 sectors—energy and utilities, communications and information technology, finance, healthcare, food, water, transportation, safety, manufacturing and government. Canada has a long-standing commitment to cyber security of critical infrastructure. It has taken a number of steps, some of which are listed below:[22]

Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) mandate: Protect the critical infrastructure from physical and cyber elements by providing national leadership.

18 *Department of Homeland Security. Retrieved from https://www.dhs.gov/critical-infrastructure-sectors*

19 *Department of Homeland Security. Retrieved from https://www.dhs.gov/national-infrastructure-protection-plan*

20 *Department of Homeland Security. Retrieved from https://ics-cert.us-cert.gov/*

21 *Department of Homeland Security. Retrieved from https://www.dhs.gov/protected-critical-infrastructure-information-pcii-program*

22 *Office of Auditor General of Canada. (2012). Protecting Canadian critical infrastructure against cyber threats. Retrieved from http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html*

National Security Policy: Prepare Canada to respond to current and future threats, including vulnerability and cyber accidents.

Canadian Cyber Incident Response Centre (CCIRC): Aim to serve as a national focal point for cyber security readiness and response as well as to deal with threats and attacks to cyber critical infrastructure.

National strategy and action plan for critical infrastructure: Enhance resilience of critical infrastructure by building partnerships and advancing the timely sharing and protection of information among partners.

Cyber Security Strategy: Tackle cyberthreats by securing government systems, securing vital cyber systems outside the federal government and helping Canadian citizens remain secure online.

United Kingdom

The UK's national critical infrastructure is categorised into 13 sectors—communications, emergency services, energy, financial services, food, government, health, transport, defence, water, civil nuclear, space and chemicals. The Centre for Protection of National Information (CPNI) has been set up to protect the national infrastructure of the UK.[23]

Centre for Protection of National Information (CPNI): It has effective relationships with private and public sector partners. In response to cyberthreats, the Government of UK has set up the Office of Cyber Security and Information Assurance (OCSIA), and the Cyber Security Operations Centre (CSOC). CPNI has worked on various other aspects such as providing documents and technical notes for raising security awareness and improving practices related to cyber ad information security.

European Union (EU)

EU has defined 11 critical infrastructure sectors—energy, information and communication technology (ICT), water, food, health, financial, public and legal order and safety, civil administration, transport, chemical and nuclear industry, and space and research. Some of the other major measures in the EU are as follows:

The European Critical Infrastructure Protection framework has been defined in order to protect these infrastructures.

European Reference Network for Critical Infrastructure Protection (ERNCIP): It provides technical support for international cyber security exercises, the assessment of the vulnerability of networked infrastructures in case of extreme space weather events, and the evaluation of the resistance of buildings and transport systems against explosions.[24]

European Programme for Critical Infrastructure Protection (EPCIP) is a package of measures aimed at improving the protection of critical infrastructure in Europe, across all EU States and in all relevant sectors of economic activity.

Joint Research Centre (JRC): The European Commission established this centre, which includes accident prevention, anti-fraud measures, crisis management, critical infrastructure protection, cyber security, global safety and security, nuclear safety, security for privacy and data protection, surveillance, and transport safety and security.

France

France has identified 12 critical sectors—civil, judicial, military, food, energy, electronic, audiovisual and information communications, space and research, finance, water management, industry, health and transportation. The following measures have been taken for protecting critical infrastructure:[25]

The **Agence Nationale de la Securité des Systèmes d'Information (ANSSI)** is a service with national responsibility and jurisdiction. ANSSI was later appointed as the French cyber defence authority.

The '**Code of Defence**' law was passed in December 2013. It gave powers to ANSSI to set minimum requirements at technical and organisational levels, mandatory cyber security incident notifications, mandatory cyber security audits and provisions for crisis management.

23 Centre for the Protection of National Infrastructure. Retrieved from http://www.cpni.gov.uk/about/cni/

24 Standards for Critical Infrastructure Protection (CIP) – The Contribution of ERNCIP. Retrieved from https://erncip-project.jrc.ec.europa.eu/standards

25 Critical Information Infrastructures Protection approaches in EU, report by ENISA. Retrieved from https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf

Australia

The Australian government has identified seven critical sector groups—banking and finance, health, food and grocery, transport, water services, communications and energy. Other measures taken are as follows:

The Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience (CIR) was established by the Australian government in 2003. It is Australia's primary national engagement mechanism for business-government information sharing and resilience-building initiatives on critical infrastructure resilience.[26]

The CIR Strategy was defined in 2015 with the aim of continuing the operation of critical infrastructure in the face of all hazards, and focusses on disaster resilience, cyber security and sector and cross-sector engagement.

Critical Infrastructure Program for Modelling and Analysis (CIPMA) was launched to assist critical infrastructure owners and operators in understanding network interdependencies and improving resilience.

India

India too realised the importance of protecting critical information infrastructure from cyberattacks and has designed multiple policies and strategies:

National Cyber Security Policy 2013: The policy aims to create a secure cyber ecosystem in the country and strengthen the regulatory framework.

The National Critical Information Infrastructure Protection Centre (NCIIPC) 2014: NCIIPC has been identified as the nodal agency under the National Technical Research Organisation for the protection of critical information infrastructure. The formal roles and responsibilities of NCIIPC include cooperation strategies, issuing guidelines, advisories and coordination with CERT-In. NCIIPC has defined controls for the critical infrastructure sectors—power and energy; banking, financial services and insurance (BFSI); ICT; transportation; and e-governance and strategic public enterprises.[27]

26 Trusted Information Sharing Network. Retrieved from http://www.tisn.gov.au/Pages/the_tisn.aspx
27 NCIIPC. Retrieved from https://nciipc.gov.in/

Some other initiatives taken by India to build cyber security and protect the critical infrastructure are as follows:

- **Computer Emergency Response Team – India (CERT-In)**
  Operational since January 2004, the Computer Emergency Response Team – India (CERT-In) is the national nodal agency for forecast, analysis and response to cyber incidents. It issues guidelines, advisories, vulnerability notes and white papers relating to the information security practices, procedures, prevention, response and reporting of cyber incidents.
- **State-level CERTs**
  States are looking at establishing individual state-level CERTs in order to fight cybercrime at a more granular level. Maharashtra and Kerala have taken the first steps in this direction.[28, 29]
- **National Cyber Coordination Centre (NCCC)**
  The National Cyber Coordination Centre (NCCC) is a proposed cyber security and e-surveillance agency.[30]

28 *Vyas, S. (2016). New weapon against cyber threat Maharashtra takes steps to establish State CERT. The Hindu. Retrieved from http://www.thehindu.com/news/cities/mumbai/new-weapon-against-cyber-threat/article8786781.ece*

29 *Kerala State IT Mission. Cyber security through CERT-K. Retrieved from http://www.itmission.kerala.gov.in/cert-kerala.php*

30 *News18. (2016). Government clears setting up of National Cyber Coordination Centre. Retrieved from http://www.news18.com/news/india/government-clears-setting-up-of-national-cyber-coordination-centre-980950.html*

5

Securing interconnected systems

Protection of the country's critical information infrastructures is of paramount importance for any government. India has already taken cognisance of the technology penetration in the critical infrastructures and the growing interconnectivity within IT, OT and CT environments. Identification of NCIIPC as the nodal agency for coordination has been a landmark in the move towards securing the critical infrastructures in the country. Taking a cue from the developments across the world, the following are some measures that can be considered for developing a robust strategy:

Security strategy and executive support

Maintaining a secure and resilient OT and CT environment requires a comprehensive strategy that covers security governance and process, implementation of the right technology and employing people with the right skills.

1. **Strategy for securing critical infrastructure:** The strategy needs to have support at the executive level, and be clearly communicated to all stakeholders. A clear understanding of cyber risks and adequate cooperation between the relevant business, IT, OT and CT teams is required.
2. **Sector-specific nodal body:** A sector-specific nodal body for designing a sector-specific plan, advisories and guidelines is significant to manage and govern the overall cyber security aspect for the sector and enhance public-private partnerships.
3. **Emergency warning network:** An emergency warning network regarding cyber vulnerabilities, threats and incidents is crucial to proactively analyse and respond to damage or attacks on such infrastructures.

Sharing and protecting information

A national strategy to secure critical infrastructures requires collaborative efforts through timely information sharing across critical sectors. Timely information on events and incidents to critical infrastructure stakeholders, for potential cross-sectoral impacts, would help in appropriate response mechanism. National-level cross-sector forums could be established to institutionalise the cooperation between various critical sectors.

Outreach and awareness programme

1. **Awareness within organisations under critical sectors**: An information security awareness programme is critical to protecting networks and assets, and organisations within each critical sector can often best achieve this by leveraging their already strong safety cultures to promote a message of 'cyber safety'.
2. **Strengthening public awareness**: Public awareness programmes need to be developed to promote public awareness and readiness to manage the impacts of disruptions.

The right cyber skills

Relevant and adequate skills are another key element to maintain the security of critical infrastructures.

1. **Skilled cyber security professionals** understand the unique challenges facing operational networks and are able to identify and communicate shortcomings in network implementation, architecture designs, technology configuration and business impact analyses. Having the right people in place will enable the organisation to prevent, mitigate, respond and recover from cyber security incidents.
2. **Continuous research and development** can help in capacity building and coming up with effective solutions. A cross-sector knowledge database inclusive of all the past incidents and threats needs to be maintained and analysed to strengthen protection measures.

Relevant, properly configured technology

Investment in the right technology is another key characteristic of resilient OT and CT networks.

1. Using the right detection, prevention, monitoring and reporting tools will help organisations to prevent attacks and facilitate informed decision-making in relation to possible cyber security threats.
2. A strong collaboration between well-equipped IT, OT and CT teams is also necessary for a unified approach to risk management and incident response.

Monitoring

OT and CT must be brought under the ambit of security monitoring, as in the case for IT networks. The periodic monitoring programme should include log monitoring, vulnerability assessments and audits of these interconnected systems. Central monitoring through nodal bodies will help in institutionalising the efforts.

Incident response

With regard to security incidents in critical infrastructure, organised efforts are required to reduce the potential cascading impact and response time. Incident response for critical infrastructures requires a partnership between public and private organisations to perform analysis, issue early warnings and coordinate response efforts.

Organisations today are more reliant on OT and CT networks to control their operations and infrastructure. Accordingly, they should build a forward-looking cyber security programme that is based on the right balance of technologies, processes and people skills—all supplemented with an ample measure of innovation. With these components in place, organisations are likely to be better prepared for the future of cyber security.

Notes

Notes

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 the 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 a '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 Indian 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 players in their 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 a balanced economic, industrial and social development. We believe education, IT, BT, health, corporate social responsibility and the 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 the management skills and expertise of professionals to set itself apart as a 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 fields of corporate social responsibility, environment and safety, HR and labour affairs, corporate governance, information technology, biotechnology, telecom, banking and finance, company law, corporate finance, economic and international affairs, mergers and acquisitions, tourism, civil aviation, infrastructure, energy and power, education, legal reforms, real estate and rural development, competency building and skill development, to mention a few.

Insight into 'new business models'

ASSOCHAM has been a significant contributor to the emergence of new-age Indian corporates, characterised by a new mindset and global ambition for dominating the international business. The chamber has addressed key areas such as promoting India as an investment destination, achieving international competitiveness, promoting international trade, corporate strategies for enhancing stakeholder value, government policies in sustaining India's development, infrastructure development for enhancing India's competitiveness, building Indian MNCs, role of the financial sector as 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. It has over four lakh direct/indirect members.

Together, we can make a significant difference to the burden that our nation carries and bring in a bright new tomorrow for our nation.

D S Rawat
Secretary General
d.s.rawat@assocham.com

ASSOCHAM
INDIA

The Associated Chambers of Commerce and Industry of India

ASSOCHAM Corporate Office:
5, Sardar Patel Marg, Chanakyapuri, New Delhi - 110 021
Tel: 011-46550555 (hunting line) • Fax: 011-23017008, 23017009
Website: www.assocham.org

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 2,08,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity in separate lines of service. Please see www.pwc.com/structure for further details.

Contacts

Sivarama Krishnan
Leader, Cyber Security
sivarama.krishnan@in.pwc.com

Siddharth Vishwanath
Partner, Cyber Security
siddharth.vishwanath@in.pwc.com

Manu Dwivedi
Partner, Cyber Security
manu.dwivedi@in.pwc.com

Sundareshwar Krishnamurthy
Partner, Cyber Security
sundareshwar.krishnamurthy@in.pwc.com

Balaji Venketeshwar
Executive Director, Cyber Security
balaji.venketeshwar@in.pwc.com

PVS Murthy
Executive Director, Cyber Security
pvs.murthy@in.pwc.com

pwc.in

PD/July2016-6922