ASSOCHAM INDIA

Contents

Securing the nation's cyberspace

pwc

www.pwc.in

Message from PwC

Sivarama Krishnan
Leader, Cyber Security
PwC India

The advancements in technology and its usage have connected people, businesses and countries and brought them closer, leading to economic progress and peace. However, these advancements come with huge vulnerabilities which can be exploited by criminals for economic gains.

Hence, it is critical that economic participants such as nation states, businesses and societies pay attention to the chinks in the armour of cyberspace, and develop adequate measures to identify, protect, detect, respond and recover processes and capabilities in the face of treats.

Cyber security in India has gained considerable momentum in the past few years. However, securing ourselves in space is not the responsibility of a single participant but one that involves all citizens, academia, enterprises, civil societies and the government. Securing cyberspace is not about deploying a few enablers such as technologies, standards, solutions or processes but a journey of social, behavioural and governance transformation supported by those enablers.

While it is convenient for citizens to relinquish all responsibility for cyber security and attempt to hold the government and corporates accountable, this is hardly a solution. Common users, in particular, need to be more attentive and diligent in their cyberspace activities. In fact, the common man can support the regulators and law enforcement agencies in managing cybercrimes if they promptly come forward to report such incidents.

To strengthen our cyber frontiers, efforts should be holistic and follow an inclusive approach involving the government, the private sector and civil society.

Message from ASSOCHAM

Sandeep Jajodia
President, ASSOCHAM

As the nation aims to connect billion people and leapfrog into next generation infrastructure, smart cities, devices and machines are getting hyper-connected across India every day. An enormous amount of real-time information is moving across the ever-expanding network at increasing speeds. The Digital India mission is going to scale this up exponentially.

Digital India will help improve the lives of hundreds of millions of people, improve governance, bring efficiency in business and enable us to compete effectively in the global economy. Such powerful capabilities come with significant vulnerabilities. The very capability that can enable e-banking, telemedicine, e-auction, e-governance and improve crop yields in seconds can disrupt life as we know it. From critical communications networks to power distribution and the financial well-being of the nation—all of these depend on the robustness of the cyber network. Each day, there are growing reports of the spread of malware, misinformation and systemic cyberattacks. These malicious forces know no physical boundaries. This is a huge challenge and needs unprecedented collective action. Indeed, cyber security is now a national priority.

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

We also convey our very best for the success of the 10th Annual Summit on Cyber & Network Security 2017.

Pratyush Kumar
Chairman, ASSOCHAM National Council on Cyber Security

Just a few days back, the honourable Supreme Court of India delivered a historic verdict that privacy is a fundamental right. The topic of this conference could not be more apt since a healthy debate and discussions on the existing data protection models and the changing technology landscape must take place. This is necessary because cyber security is no longer only an information technology problem. It has the potential to impact individuals, businesses and the economy.

Imagine a vibrant Digital India which is expected to improve the lives of hundreds of millions of people and governance, bring efficiency in business, and enable us to compete effectively in the global economy. Such a powerful capability also comes with significant vulnerabilities. The very capability that can enable e-banking, telemedicine, e-auction, e-governance and improve crop yields can disrupt life as we know it in seconds. The rate of cybercrime in India has increased in 2017. Now, it is estimated that one case of cybercrime is reported every 10 minutes in India. The digital revolution in India is expected to impact the common man profoundly as it is related to day-to-day activities—banking, buying goods and services, transferring money, etc. Therefore, it is important that a robust cyber security framework is in place that assures the common man that his/her identity will not be compromised. These malicious forces know no physical boundaries. This is a huge challenge and needs unprecedented collective action. Indeed, it is now a national priority.

As we discuss the right mechanism to deal with this threat, let's also acknowledge that there are multiple stakeholders in the cyber security domain—governments, private product and service companies, and Internet service providers. Hence, we should strive to develop a holistic mindset towards cyber security challenges that takes into account the requirements of all stakeholders and does not focus on developing 'point' solutions.

In the past few years, we have seen a negative impact of cyberattacks on the geopolitical stage. In that context, it is heartening to know that the Indian government is taking measures to strengthen its cyber security arm and protecting the Indian cyberspace and software infrastructure against destructive hacking activities. Clearly, a big responsibility rests with all private parties to collaborate with the government to craft a regulation that is mandatory for every entity touching the data without 'over-regulating' the industry that is expected to deliver significant economic benefits to India. Regulations

such as the General Data Protection Regulation (GDPR), which harmonises data protection regimes, are a good starting point to conceptualise how similar regulations can be crafted for India. The Government of India has launched several initiatives, such as Indian Computer Emergency Response Team (ICERT) and Reserve Bank Information Technology Pvt Ltd (ReBiT), which reflect their intention, but now there is a need to complement the regulations.

No other sector in India is as vulnerable to a shortage of trained and skilled human resources as cyber security. The shortage of qualified and skilled people that understand the nuances of technology in order to deal with the exponentially growing data transactions is alarming. Specifically, we should be working tirelessly on reducing shortages among law enforcement agencies. It's ironic that India produces 1.2 million engineers every year and exports IT services worth 80 billion USD to the world and yet lags behind in developing a skilled pool of cyber protectors as law enforcement officers, nodal agency staff and regulators. Without a skilled talent pool, we won't be able to develop 'world-class' government institutions (regulators and nodal bodies) to ensure cyber security.

Collaboration improves everyone's cyber security preparedness. At ASSOCHAM, we are striving to achieve multifaceted collaboration across the government, industry, academia and civil society. ASSOCHAM participates in the Joint Working Group (JWG) on Cyber Security set up by the National Security Council Secretariat (NSCS), Government of India, and is a Member of the Cyber Regulation Advisory Committee and the Joint Working Group on Digital India, both set up by the Ministry of Communications and IT, Government of India. Leading Indian and global companies are members of ASSOCHAM's Cyber & Network Security Council.

Cyberspace and network security is by nature international, even when viewed from a national security lens. Therefore, it will require a partnership between people, businesses, governments and nations.

The 10th edition of the Cyber & Network Security Summit presents a unique opportunity for a dialogue among all key stakeholders—governments, industry, academia, and civil society—to face the faceless enemy that stands before us.

Debu Nayak
Co-Chair, ASSOCHAM National Council on Cyber Security

As co-chair of the ASSOCHAM Cyber Security Council, I find the topic of this summit to be very timely and relevant. The summit will be extremely useful to all policymakers, industry leaders and citizens. I wish the summit great success.

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 of cyberattacks and malware is not only apparent but also very worrisome. There cannot be a single solution to counter such threats. A good combination of law, people, process and technology must be established and then an effort be 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 on 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 on Cyber Security set up by the National Security Council Secretariat (NSCS), Government of India; a member of the Cyber Regulation Advisory Committee and of the Joint Working Group on Digital India, both set up by the then 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 on their efforts.

We convey our very best wishes for the success of the 10TH ASSOCHAM Annual Summit: Cyber & Network Security'. The theme for this year's summit is 'Protecting Our Nation against Faceless Enemies' and we hope that it provides more insight into the emerging cyber-related challenges and solutions for further securing cyberspace.

Making the nation cyber secure

Unprecedented growth in technology has blurred boundaries by connecting people and transforming the way we work and how governments serve their citizens. Digitisation is enabling the youth to work from their villages, enabling people to talk at seminars and attend family functions remotely, perform digital darshan, transfer money to near ones instantly and much more. The Digital India Programme launched by the Government of India, which aims to provide government services digitally and promote digital literacy, besides building secure digital infrastructure for the country, is driving this transformation.

Digital payments have also seen an upsurge, with mobile banking transactions alone growing threefold since 2014. It is envisaged that with these initiatives in place, India's digital economy will grow from 270 billion USD to around 1 trillion USD in the next 5–7 years.[2]

However, this is also opening up gaps which can be exploited by the adversaries and deprive us of the benefits of digital technologies. The number of incidents reported by the Indian Computer Emergency Response (CERT-In) was 27,482 till June 2017. Cyber adversaries are becoming more sophisticated and resourceful, the impact of cybercrime is increasing, and the attacks are increasing not only in volume but also in variety. Among more than 100 countries that were hit by WannaCry (an advanced ransomware attack),[3] India was the third worst affected.

Digital trends in India[1]

1.1 billion telephone subscribers
2nd largest in world

241 million Facebook users
Social media penetration

1.15 billion digital IDs
Largest national ID programme

463 million Internet users
2nd largest in the world

Cyberattacks can deliver economic blows, derail India from its projected growth trajectory and worsen relations with our neighbours, unleashing a state of anarchy. Considering both the benefits of technology and the need to safeguard against cyberattacks, it is imperative for a growing digital economy like India to focus on cyber security and build a cyber-resilient environment.

1 TRAI (2017). Economic Times. Retrieved from http://trai.gov.in/sites/default/files/Press_Release_No50_Eng_13072017.pdf (last accessed on 25 Aug 2017)
UIDAI (2017). Retrieved from https://uidai.gov.in/ (last accessed on 23 Aug 2017)
Francisco, S. (2017). India becomes Facebook's largest user base with 241 mn users, overtakes US. Retrieved from http://www.business-standard.com/article/current-affairs/india-becomes-facebook-s-largest-user-base-with-241-mn-users-overtakes-us-117071400251_1.html (last accessed on 23 Aug 2017)
Internet Stats. Retrieved from http://www.internetlivestats.com/internet-users/india/
Bhakta, P. (10 Aug 2017). Digital transactions in July touch 859.2 million. Economic Times. Retrieved from http://economictimes.indiatimes.com/industry/banking/finance/banking/digital-transactions-in-july-touch-859-2-million/articleshow/59994667.cms
Electronic Transaction Aggregation & Analysis Layer. Retrieved from http://etaal.gov.in/etaal/auth/login.aspx (last accessed on 23 Aug 2017)

2 Financial Express Bureau. (24 May 2017). India's digital economy set to grow from $270 bn to $1 tn by 2024, says Ravi Shankar Prasad. Financial Express. Retrieved from http://www.financialexpress.com/economy/indias-digital-economy-set-to-grow-from-270-bn-to-1-tn-by-2024-says-ravi-shankar-prasad/682805/ (last accessed on 23 Aug 2017)

3 Kumar, C. (14 May 2017). Ransomware attack hits at least 100 systems in India. Retrieved from http://timesofindia.indiatimes.com/india/ransomware-attack-hits-at-least-100-systems-in-india/articleshow/58663696.cms (last accessed on 23 Aug 2017)

Key cyber security initiatives launched by the Government of India

As forward-looking nation, India has taken some initiatives to strengthen its cyberspace. These include awareness programmes; efforts to create a strong policy environment and strengthen security monitoring capabilities, and international cooperation; and research and development to promote cyber security. Some of the key initiatives are mentioned below under:

1. **National Cyber Security Policy:** The policy provides the vision and strategic direction to protect the national cyberspace. The policy was released in 2013.
2. **National Cyber Security Coordination Centre (NCCC):** The NCCC will perform real-time threat assessment and create situational awareness of potential cyberthreats to the country. It was made operational in August 2017.
3. **National Critical Information Infrastructure Protection Centre (NCIIPC):** The organisation was created under section 70A of the IT Act. It is designated as a national nodal agency in respect of critical information infrastructure protection. It aims to protect and safeguard critical information infrastructure (CII) against cyberterrorism, cyberwarfare and other threats.
4. **Cyber Swachhta Kendra:** Launched in early 2017, the Cyber Swachhta Kendra provides a platform for users to analyse and clean their systems of various viruses, bots/ malware, Trojans, etc.[4]
5. **International cooperation:** Seeking to secure cyberspace, India has entered into nine[5] new bilateral agreements with developed nations such as the US, Singapore and Japan in order to promote research and information sharing on cyber security. These collaborative efforts will enable India to combat advanced threats.
6. **Promoting research and development:** To promote cyber security across the nation, the government has initiated a programme to offer a public grant worth 5 crore INR to companies responsible for innovation and research in cyber security.
7. **Sectoral and state CERTs:** The government has launched sectoral CERTs, starting with critical sectors such as power and finance. Further, state-level CERTs are expected to be created.[6]
8. **Security testing:** There are plans to set up 10 additional Standardisation, Testing and Quality Certification (STQC) testing facilities across the country for the evaluation and certification of IT products.

According to the International Telecommunication Union's (ITU) Global Cyber Security Index, India ranked 5th in 2015, but has moved to the 23rd rank among 134 countries in 2017.[7] The security landscape of the country may be further improved with concrete initiatives and learnings from other countries.

4 PIB (2017). Press release. Retrieved from http://pib.nic.in/newsite/printrelease.aspx?relid=158620

5 The Center for Internet & Society. (2016). Mapping of India's cyber security-related bilateral agreements. Retrieved from https://cis-india.org/internet-governance/blog/india-cyber-security-bilateral-agreements-map-dec-2016 (last accessed on 23 Aug 2017)

6 PIB (2017). Press release. Retrieved from http://pib.nic.in/newsite/printrelease.aspx?relid=158620

7 International Telecommunication Union. (2017). Global Cybersecurity Index. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (last accessed on 23 Aug 2017)

Building blocks for a secure nation

Based on an analysis of 60+ countries performed by PwC, the national cyber security strategy is categorised into four building blocks to provide holistic coverage and sufficient focus.

Building a cyber secure nation

1 Securing government systems	2 Securing business cyber ecosystem	3 Creating cyber secure society
Protection of government assets, infrastructure and systems from cyber threats is paramount for the upkeep of our socio-economic health and military might. It is vital for safety, security, growth and sustenance of the nation's economy, protection of its citizens, wealth and infrastructure.	A healthy and resilient cyber ecosystem is required for the enterprises to effectively contribute in the progress of the nation. For this to succeed, all the stakeholders need to collaborate to cohesively contribute to security	A society driven by cyber safe culture is less susceptible to cyber adversaries. Creating awareness and training people on cyber security are required to attain a true cyber secure society.

4 Building technological and human capacity

Creation of indigenous tools & human capacity and capability is imperative to not only protect Indian cyber space but also to make India globally competitive in cyber security.

A robust cyber security approach requires adequate proactive and reactive measures to identify, protect, detect, respond and recover processes across these four building blocks.

Approach for holistic cyber security

Proactive			Reactive	
Identify	Protect	Detect	Respond	Recover
Develop the organisational understanding to manage cyber security risk to systems, assets, data, and capabilities	Develop and implement the appropriate safeguards to protect or deter cyber security threats	Implement continuous monitoring to provide proactive and real time alerts of cyber security related events	Develop and implement the appropriate activities to take action regarding a detected cyber security event	Develop and implement the appropriate business continuity plans to maintain resilience and recover capabilities after a cyber breach

Building block 1: Securing government systems

Securing government assets, infrastructure and systems from cyberthreats is paramount for the upkeep of our socio-economic health and military might. It is vital for the safety, security, growth and sustenance of the nation's economy, protection of its citizens and its wealth and infrastructure. Given the sensitivity of data residing with the government, the security of government systems is of utmost importance.

Learnings from other countries

Countries across the globe have taken measures to improve the security of their governments' infrastructure.

EINSTEIN System, Department of Homeland Security (DHS), US: EINSTEIN serves two key roles in federal government cyber security. First, EINSTEIN detects and blocks cyberattacks from compromising federal agencies. Second, it provides DHS with the situational awareness to use threat information detected in one agency to protect the rest of the government and to help the private sector protect itself. EINSTEIN provides perimeter defence for federal civilian executive branch agencies. By the end of 2016, 93% of federal users were covered under this programme.[8] This helps in the generation of useful and actionable intelligence, thus helping administrators in identifying the emergencies and priorities and offering information on effective configuration, other than helping US-CERT in generating cross-governmental trend analysis.[9]

Centre for Protection of National Infrastructure (CPNI), UK: CPNI provides security advice targeted primarily at the critical national infrastructure, where compromise or loss would result in detrimental impacts on the essential services of the country.[10] The UK has defined 13 national infrastructure sectors and each sector has one or more lead government department(s) (LGD) responsible for the ensuring security of critical assets. Further, within the national infrastructure sector, they have defined specific assets as 'critical', whose loss or compromise would result in detrimental impacts on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or the loss of life.[11]

Continuous Diagnostics and Mitigation (CDM) programme, DHS, US: Federal agencies have been directed to implement continuous monitoring of their IT assets and operational environments. It calls for a three-tiered approach to risk management through defined standards and guidance across organisations, mission/business process and information systems by covering 15 continuous diagnostic capabilities. CDM offers commercial off-the-shelf tools to federal agencies to identify cyber security risks on an ongoing basis, prioritise them based on potential impact and enable their mitigation.[12]

National Cyber security and Communications Integration Centre (NCCIC), DHS, US: As part of the DHS's information-sharing initiative, NCCIC works with the government and private sector to provide a unified response to cyber incidents. NCCIC integrates the United States Computer Emergency Readiness Team (US-CERT), Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), National Coordinating Centre NCC), NCCIC Cyber Operations Centre (COC), Discovery and Technical Analysis (DTA) and Mission Management (MM).[13] It maintains a common cyber platform which provides cross-domain situational awareness for cyber risk.[14] [15]

8 Executive Office of the President of the United States. Federal Information Security Modernization Act of 2014. Annual report to congress. Retrieved from https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report to_congress_official_release_march_10_2017.pdf (last accessed on 23 Aug 2017)

9 DHS. (2017). EINSTEIN. Retrieved from https://www.dhs.gov/einstein (last accessed on 23 Aug 2017)

10 Centre for the Protection of National Infrastructure. Retrieved from https://www.cpni.gov.uk/about-cpni

11 CPNI. (n.d.) Critical National Infrastructure. Retrieved from https://www.cpni.gov.uk/critical-national-infrastructure-0 (last accessed on 23 Aug 2017)

12 DHS. (2017). CDM.. Retrieved from https://www.dhs.gov/cdm# (last accessed on 23 Aug 2017)

13 Zelvin, L. (n.d.). NCCIC. [Presentation]. Retrieved from http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-10/ispab_oct2012_lzelvin_nccic-overview.pdf (last accessed on 23 Aug 2017)

14 DHS. (2017). NCCIC. Retrieved from https://www.dhs.gov/national-cybersecurity-and-communications-integration-center (last accessed on 23 Aug 2017)

15 National Cybersecurity and Communications Integration Center. Retrieved from https://www.hsdl.org/?view&did=780083

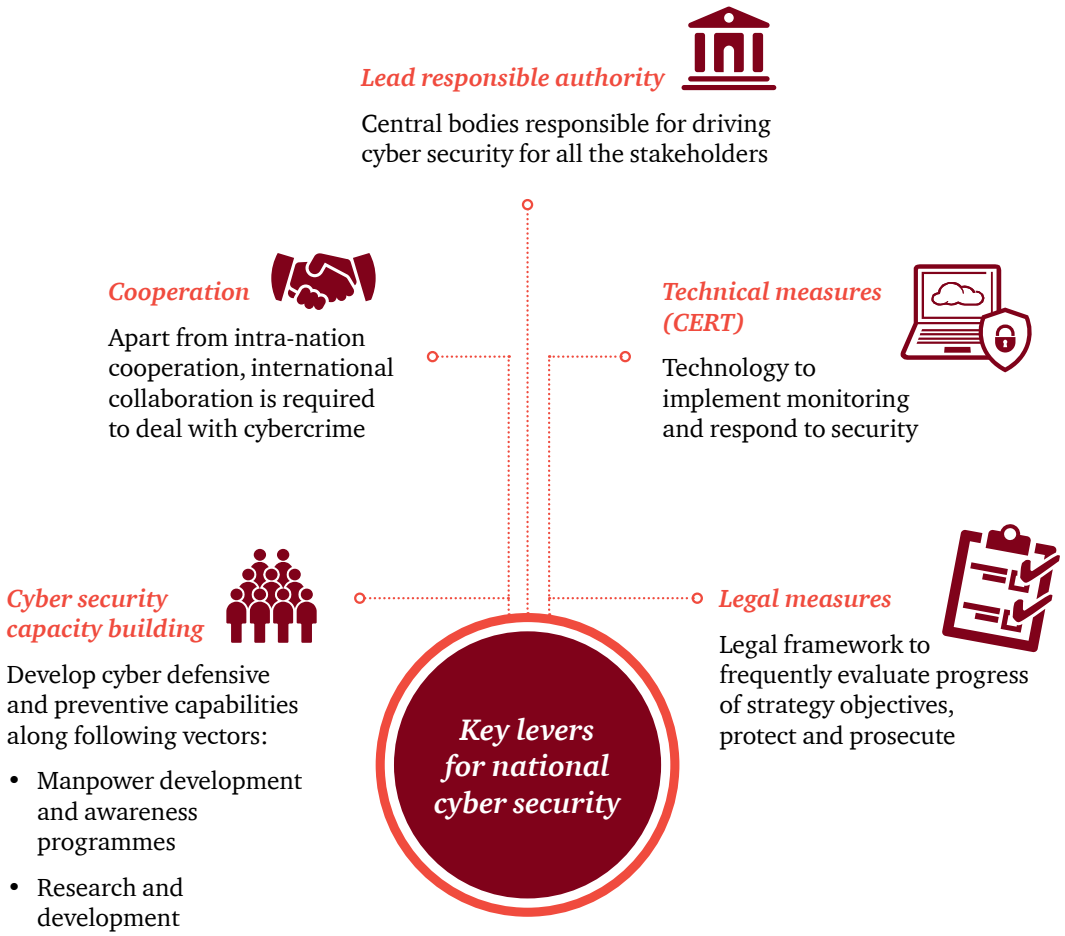
Cyber Star Exercise, Singapore: The Cybersecurity Agency of Singapore (CSA) conducts the cyber star exercise to test the cyber incident management and emergency response plans of Singapore. The scope of this exercise covers all eleven designated critical information infrastructure (CII) sectors in Singapore. This helps in improving the tiered national cyber security response plan which allows for timely response and ground initiatives at the local, sectoral and national level.

Hack Department of Homeland Security Act, US: Introduced in 2017, the act establishes a 'bug bounty programme' to encourage people to come forward and report vulnerabilities in the government infrastructure. The main objective of this act is to incentivise ethical hackers to report gaps and vulnerabilities in federal systems before others do.[16]

Mobile Incident Response Team, Germany: The National Cyber Security Strategy of Germany for 2016 mandates the creation of a Mobile Incident Response Team (MIRT).[17] MIRT is a specialist cyber task force that will provide rapid on-site assistance to address serious cyber security threats on request and with the consent of federal authorities and operators of critical infrastructure.[18]

Despite variations, common threads exist in the National Cyber Security Strategy (NCSS) key strategy implementation levers of most nations.

Key levers for national cyber security



16 Congress.gov. S.1281 - Hack DHS Act. Retrieved from https://www.congress.gov/bill/115th-congress/senate-bill/1281/text (last accessed on 23 Aug 2017)

17 BSI. (2016). National Cyber Security Strategy2016 . Retrieved from https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/meetings/april-2017/170426-bsi-enisa-nlo-presentation-v2.pdf (last accessed on 23 Aug 2017)

18 Federal Office for Information Security. (2017). Security in focus. Cyber security strategy for Germany 2016. BSI Magazine 2017. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2017-01.pdf?__blob=publicationFile&v=4 (last accessed on 23 Aug 2017)

Call to action

We believe that governments should focus on three areas, namely creating a robust policy environment, building capacity and ensuring adequate technology support for government systems.

1

Governance, policies, procedures and guidelines

- Prescribe detailed policies, procedures and standards encompassing all government infrastructure to provide clear definitions and interpretations of security objectives to be implemented.
- Create and support the building of capacities within user organisations on security skills development and enhancement.
- Conduct periodic and mandatory security assessments of government organisations and their ecosystems to maintain security postures and hygiene.
- Enforce all government departments to report data security breaches compulsorily to nodal agencies.
- Define third-party vendor guidelines for secure cyber practices and adherence to policies, procedures and standards defined.
- Define processes for continuous and real-time monitoring of all IT assets, interconnected networks and operational environments through a central Security Operations Centre (SOC) with advanced analytical capabilities.

2

Build capacities and capabilities in people to practice security

- Include security-related skills in the job descriptions of government employees by working in close coordination with the Department of Personnel and Training (DoPT).
- Identify and build cyber security skills to protect information systems and assets.
- Periodically brief senior personnel on existing and emerging cyberthreats, trends and directives.
- Create cyber awareness across government organisations and its employees.
- Initiate a bounty programme among citizens to report gaps and vulnerabilities in government systems.
- Grant security clearance and non-disclosure agreements (NDAs) for third parties, vendors working for critical establishments.

3

Technology to prevent, detect, respond and recover

- Define minimum security features for the hardware and software to be deployed in the government ecosystem
- Define security reference architecture to be implemented by all government departments.
- Build capabilities and capacity for application, equipment and infrastructure testing through the deployment life cycle to detect any vulnerability and backdoors in the product/technology.
- Design, develop, implement and operate Security Operations Centre for the government with capabilities to detect, respond and recover from any breaches and attacks.
- Strengthen CERT-IN processes and infrastructure for incident response and recovery capabilities to act proficiently on requests from state and central departments/agencies.
- Assess creation of shared data repository infrastructure similar to a secure cloud, to support on-demand requirements of various government agencies to push or pull data.

Building block 2: Securing the business cyber ecosystem

Businesses today face a quandary in today's world of fierce competition. Efficiency, speed to market and customer centricity take precedence, while protection of one's digital assets takes a backseat. However, in this era of digitisation, it is imperative to have a balance between these levers.

There is a need to provide a secure business cyber ecosystem, where governments and national agencies can provide support through an adequate regulatory environment and oversight, while businesses not only follow mandates but help in creating self-regulated environments.

Learnings from other countries

Sector-specific standards: The US DHS has released specific cyber security guidelines for the manufacturing sector, in addition to the National Institute of Standards and Technology's (NIST) cyber security framework.[19] Such frameworks also exist for the energy, transportation and the emergency services sector, etc. Laws, regulatory mandates and standards tailored to sector-specific requirements have been created such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH) Act for the healthcare sector and the North American Electric Reliability Corporation – critical infrastructure protection (NERC CIP) for the energy sector.

Regulatory bodies: The Monetary Authority of Singapore **(MAS)**, as a regulator, released specific guidelines for strengthening system security and risk management for technology-enabled systems of financial institutions within the country. Guidelines have been detailed for the identification and mitigation of risks across broad processes involved in the design and implementation of IT systems.[20] Similar guidelines are also released by the Australia Prudential Regulatory Authority (APRA).

Sectoral Information Sharing and Analysis Centres (ISACs), US: The US has also spearheaded the formation of various sectoral ISACs, especially for critical infrastructure. The ISACs collect, analyse and disseminate actionable threat information to its various members along with tools to mitigate the identified risks. There are currently more than 20 such ISACs in the US which have collaborated with each other and federal agencies on joint advisories, white papers and reports, as well as national-level exercises with the DHS and the Foreign Exchange Management Act.[21]

National Cyber Response Coordination Group (NCRCG), US: It serves as the US government's principal mechanism to facilitate coordination of efforts to respond to and recover from cyber incidents of national significance. NCRG coordinates with various bodies such as the US-CERT, Homeland Security Operations Centre (HSOC) and leverages existing resources for coordination and outreach activity.[22]

Protected Critical Infrastructure Information (PCII) Programme, US: Established in response to the Critical Infrastructure Information (CII) Act of 2002, the PCII programme is an information protection programme to enhance information sharing between the private sector and the government. Formulated to protect critical infrastructure from cyberattacks, PCII is used by DHS and other government security professionals to assess and enhance security of critical infrastructure and take appropriate measures. Under the programme, federal, state and local government employees and their contractors can access PCII only if they meet a defined set of requirement.[23]

Government Forum of Incident Response Security Teams (GFIRST), US: GFIRST comprises a group of tactical and technical security response teams who work together to understand and handle computer security incidents and encourage proactive and preventative security practices.[24]

National Cyber Security Drill, Korea: Korea's CERT and Coordination Centre (CC) have been organising cyber security drills for the past 10 years with the aim of testing for security vulnerabilities and developing the capabilities of stakeholders in handling cyberthreats.[25]

19 DHS. (2015). Critical manufacturing sector cyber security framework implementation guidance. Retrieved from https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/critical-manufacturing-framework-implementation-guide-2015-508.pdf (last accessed on 23 Aug 2017)

20 MAS. (2013). Technology risk management guidelines. Retrieved from http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf (last accessed on 23 Aug 2017)

21 National Council of ISACs. ISACs and their role in critical infrastructure protection. Retrieved from https://docs.wixstatic.com/ugd/416668_2e3fd9c55185490abcf2d7828abfc4ca.pdf (last accessed on 23 Aug 2017)

22 US-CERT. (n.d.). National Cyber Response Coordination Group. Retrieved from https://www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf (last accessed on 23 Aug 2017)

23 DHS. (2017). PCII programme. Retrieved from https://www.dhs.gov/sites/default/files/publications/pcii-fact-sheet-2017-508.pdf (last accessed on 23 Aug 2017) PCII programme. (n.d.). Non-disclosure of protected CII. Retrieved from https://www.dhs.gov/xlibrary/assets/pcii_faqs.pdf (last accessed on 23 Aug 2017)

24 US-CERT. (n.d.). GFIRST. Retrieved from https://www.us-cert.gov/government-users/collaboration/gfirst (last accessed on 23 Aug 2017)

25 Sung Jung, M. (28 March 2017). How to organize a national cyber security drill. [APNIC]. Retrieved from https://blog.apnic.net/2017/03/28/organize-national-cybersecurity-drill/ (last accessed on 23 Aug 2017)

Cleaner Internet initiative, Singapore: The Infocomm Development Authority (IDA) of Singapore issued the Secure and Resilient Internet Infrastructure Code of Practice (SRII-CoP) in 2011. This code, under the telecommunications regulatory framework, allows Internet service providers (ISPs) and the IDA to make more informed decisions so that early warning to emerging cyberthreats can be developed and appropriate pre-emptive measures can be taken. This was further extrapolated in Singapore's Cybersecurity Strategy that ISPs should to ensure a cleaner Internet and should function as gatekeepers, managing gateways and enabling information flow across the Internet.[26]

Call to action

We believe an inclusive approach is required to create a secure business ecosystem, where the government, industry sectors, standard bodies and business all have to play their role in creating a secure environment.

1

Sectoral regulator

- Identify the critical assets and processes as well as risks emanating from them.
- Mandate industry-specific processes, guidelines, standards and reference security architecture.
- Prepare and communicate guidelines for incident detection, mitigation and response.
- Create an ecosystem for independent validation and verification of security controls applicable to an entity.
- Mandate the formation of sectoral CERT and drive its operations to ensure security across various entities.
- Create a platform for cyber security information sharing and knowledge transfer among entities in a particular sector as well as across sectors.
- Mandate necessary disclosure of the incidents or breaches in a particular entity in a timely manner.
- Define third-party vendor guidelines for secure supply chain practices such as having NDAs, background checks and relevant security certifications.
- Conduct cyber drills and large attack simulation exercises.

2

Government

- Create a sector-specific platform with the regulator to coordinate security activities.
- Extend technical and investigative support to entities in the event of a cyber security incident or breach.
- Facilitate coordination and cooperation between sector-specific entities and entities in other sectors for security intelligence sharing.
- Promote organisations or entities that adopt security practices through some sort of funding or incentives.
- Define the reporting guidelines and subsequent disciplinary actions and guidelines for entities in the event of a lapse in security on an organisation's part.
- Promote and assist the standards body to enable them to make sector-specific standards and guidelines.
- Encourage small and medium sector enterprises to adopt cyber security practices by providing incentives.

26 IDA. (n.d.). National cyber security masterplan 2018. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Singapore_2013_AnnexA.pdf (last accessed on 23 Aug 2017)

3

Standard bodies

- Build the capacity and capability of the standard body to develop sector-specific standards.
- Engage industry bodies, academia, the government and law enforcement agencies to develop and define standards, mechanisms and guidelines which are in sync with the requirements of the industry.
- Facilitate the deployment of standards across various entities in a particular sector by building an ecosystem for its smooth compliance and implementation by handholding organisations to achieve their objectives.
- Sustain and maintain standards on a regular basis by updating them to ensure they remain consistent with technological innovation and security practices.

Building block 3: Creating a 'cyber secure society'

Citizen participation is key to make any initiative a great success. Responsible behaviour of citizens can pave the way for a strong foundation to create a cyber-safe culture and secure a nation's cyberspace. A society driven by such a cyber-safe culture will be far less prone to cyberattacks.

There is a need to sensitise both enterprises and citizens regarding their rights and obligations when in a cyberspace. Awareness about secure online behaviours and training people on cyber security topics and best practices can help in protecting people from falling prey to cyber criminals, thus leading to the formation of a secure cyber society.

Learnings from other countries

Cyber Aware, UK: A cross-government awareness campaign to drive behavioural change among businesses and individuals delivered by the Government of UK (Home Office) in conjunction with the Department for Digital, Culture, Media & Sport alongside the National Cyber Security Centre. For wide outreach, this campaign is run using social media.

Stop. Think. Connect Campaign, US: Conducted under the DHS, this initiative is a national public awareness campaign to increase the understanding of cyberthreats and empower the American public to be safe and secure online.[27] The key objectives of the campaign include elevating the nation's awareness of cyber security, engaging the public and communicating approaches and strategies for the upkeep of public safety online. It is associated with nearly 100 network partners to propagate cyber security awareness.

Massive Online Open Courses (MOOCs), UK: MOOCs are offered throughout the year. These are fast becoming popular in the UK as a medium of spreading cyber security awareness among the masses.[28] More than 25 of UK's universities have begun offering cyber security courses.

Office of the eSafety Commissioner, Australia: Australia's Office of the eSafety Commissioner provides a range of information and resources designed to meet the cyber safety needs of children, parents and teachers.[29]

- **Pre-service teacher programme:** This programme provides training and education to teachers about cyber safety and enables them to suitably educate their students.
- **Virtual classrooms:** These classrooms cover issues such as cyber bullying, communicating online, the Internet and law, and digital rights and wrongs and cater to children based on their age groups.

ThinkUKnow, Australia: This is Australia's first nationally delivered crime prevention programme. All Australian police forces are part of the ThinkUKnow cyber safety programme. It provides cyber safety presentations that are aimed at parents, teachers and children from grades 3–12, covering a range of topics including sexting, cyber bullying and online child exploitation.[30]

Call to action

1

Building a cyber secure society

- Encourage and enforce ISPs to provide clean Internet to citizens, which is devoid of any virus/ botnet/DDoS malwares.
- Involve the community, civil society, non-profit organisations in spreading cyber security awareness and expanding the reach by identifying the cyber security awareness champions for respective organizations and communities.
- Mandate schools and colleges to provide basic cyber security training to students.
- Decide the most appropriate mode of dissemination of cyber security-related awareness material through social media, MOOCs, electronic and print modes, street plays, etc.
- Organise national- and international-level seminars and workshops in association with industry bodies.

27 DHS. (2016). Stop. Think. Connect. Retrieved from https://www.dhs.gov/stopthinkconnect (last accessed 23 Aug 2017)

28 Cyber degrees. (n.d.) Free online cyber security courses (MOOCs). Retrieved from http://www.cyberdegrees.org/resources/free-online-courses/ (last accessed on 23 Aug 2017)

29 Office of the eSafety Commissioner. Retrieved from https://www.esafety.gov.au/ (last accessed on 23 Aug 2017)

30 ThinkUKnow. Retrieved from https://www.thinkuknow.org.au/ (last accessed on 23 Aug 2017)

Building block 4: Building technological and human capacity for cyber security

New innovation and cyber norms should focus efforts on creating both capabilities and capacities to defend against latest cyberthreats emerging from paradigm shifts in technology. With the ever-expanding cyberspace, attackers are exploring new and innovative ways to attack technology infrastructure. Indigenous technologies also provide the additional assurance of being secured against vulnerabilities/ backdoors in custom products. In addition to technological capabilities, it is imperative to have trained manpower to implement the necessary cyber strategies.

To build technological and human capacities, emphasis should be laid on the creation of niche tools and a workforce that protects the Indian cyberspace.

Learnings from other countries

Research and development (R&D) through cyber security clusters

Several countries across the globe have established cyber security 'clusters' to foster innovation and promote research and development in the field. These clusters are areas with a high concentration of cyber security companies with special incentives and growth accelerators. Some of these cyber security clusters are described below:

Cyber cluster	Number of cyber security companies	Salient features
Greater Baltimore Cluster, US	10,000+	• Government initiatives such as the **System for Award Management (SAM), NSA's Small Business Office, FedBizOpps,** etc., have helped boost the local industry and have encouraged private contractors to enrol as federal suppliers. • Public-private partnerships (PPPs) for **commercialisation of intellectual property** have helped with the development of niche products.
Hague Security Delta (HSD), Netherlands	400+	• Promoted collaboration with industry, academia and the government. Created vision 2020 that is focused on making innovation the centre for cyber security, bringing diversity in the field of security (at least 20%) and enhancing partnerships with other clusters.
Beersheva, Israel	250+	• Attracted about 20% of global private sector investment in the cyber security industry. • Leading technology companies have setup up Centres of Excellence in the city in collaboration with Ben-Gurion University of the Negev. • It also has dedicated funds for cyber security such as Jerusalem Venture Partners (JVP) cyber labs.
Berlin-Brandenburg cluster, Germany	250+	• Established cooperative networks, such as security and safety made in Berlin-Brandenburg (SeSamBB), which comprises security experts from multinational corporations, SMEs and university research institutions for interdisciplinary projects in internal and public security.
Ottawa security cluster, Canada	180+	• Files many patents in the aerospace, defence and security sectors.
UK cyber security clusters	600+	• Focused on research and development in the field of cyber security.

Law Enforcement Cyber Centre (LECC), US: LECC assists law enforcement, including police officers, digital forensic investigators, detectives and prosecutors to investigate and prevent cybercrime. Some of the programmes include:

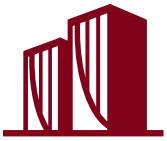
- **FBI Cyber Investigator Certification programme:** This is a multi-level online training programme that is designed to teach advanced technical skills.[31]
- **National Initiative for Cybersecurity Careers and Studies (NICCS):** The main objective of the NICCS is to grow the cyber workforce through a robust, searchable catalogue that allows users to find cyber training programmes based on location, delivery method and specialty area.[32]
- **Computer Crime and Intellectual Property Section (CCIPS):** CCIPS provides training to state and local law enforcement, prosecutors and government officials. These trainings are available as online courses and cover various topics such as cybercrime, privacy, computer forensics and electronic transactions.[33]

College of Policing, UK: It works with the police services in England and Wales to provide cyber training and awareness for investigators to increase their ability to understand and respond to cybercrime. Major subjects include managing victims of cybercrime, case file preparation for digital evidence and investigative opportunities of the dark web.[34]

Call to action

1

Capacity building



- Encourage schools, universities and colleges in defining cyber security courses and subjects.
- Organise summer schools/specialised coaching for students to make them aware of and to promote cyber security.
- Offer scholarships for students pursuing courses in cyber security, specifically those conducting doctorate research in the field of cyber security.
- Organise cyber security-related challenges and competitions at a national level to generate interest and find innovative solutions to cyber security issues.
- Establish cyber security training infrastructure for awareness and skill development. These could also be built by private organisations and could be adequately certified by the government
- Ensure cyber capacity building for law enforcement agencies as well as its personnel.

2

Promoting research and development

- Set up investment funds focused on cyber security initiatives/ start-ups.
- Offer tax incentives and subsidies to cyber security start-ups.
- Create incubation and research centers in collaboration with academia and industry.
- Induce domestic market demand by focusing on key purchasers (e.g. the government, defense, banking, financial services and insurance [BFSI], etc.)
- Create platforms for start-ups to demonstrate their cyber security innovation and technology.

31 Cyber Investigator Certificate Programme. Retrieved from https://fbi-cicp.cert.org/lms/ (last accessed on 23 Aug 2017)

32 DHS. (2013). DHS launches NICCS. Retrieved https://www.dhs.gov/news/2013/02/21/dhs-launches-national-initiative-cybersecurity-careers-and-studies (last accessed on 23 Aug 2017)

33 The United States Department of Justice. (n.d.). CCIPS. Retrieved https://www.justice.gov/criminal-ccips (last accessed on 23 Aug 2017)

34 College of policing. Retrieved from http://www.college.police.uk/Pages/Home.aspx (last accessed on 23 Aug 2017)

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 the 'knowledge-based economy'.

ASSOCHAM is seen as a forceful, proactive and 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 and 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 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 contributory factor in the emergence of new-age Indian corporates, characterised by a new mindset and global ambition for dominating the international business. The chamber has addressed itself to key areas like India as an 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, and the role of the 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, and has over 4 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 2,23,000 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

Anirban Sengupta
Partner, Cyber Security
anirban.sengupta@in.pwc.com

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

Murali Talasila
Partner, Cyber Security
murali.talasila@in.pwc.com

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

Rahul Aggarwal
Partner, Cyber Security
rahul2.aggarwal@in.pwc.com

Ram Periyagaram
Partner, Cyber Security
ram.periyagaram@in.pwc.com

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

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

Unnikrishnan Padinjyaroot
Partner, Cyber Security
unnikrishnan.padinjyaroot@in.pwc.com

Hemant Arora
Executive Director, Cyber Security
hemant.arora@in.pwc.com

Krishna Sastry Pendyala
Executive Director, Cyber Security
sastry.pendyala@in.pwc.com

Sriram S
Executive Director, Cyber Security
sriram.s@in.pwc.com

pwc.in

Data Classification: DC0

AW/August2017-10541