Strategic national measures to combat cybercrime:
Perspective and learnings for India
August 2015
Contents

1. India: current cybercrime landscape and leading practices across globe -------------- 07
   1.1 National level plan/strategy--------------------------------------------- 07
   1.2 Responsible agencies/departments-------------------------------------- 10
   1.3 Legal measures---------------------------------------------------------- 11
   1.4 Training and awareness----------------------------------------------- 13
   1.5 Cybercrime reporting mechanism---------------------------------- 15
   1.6 International collaboration to thwart cybercrime---------------- 16
   1.7 Capacity building for strong cybersecurity---------------------- 18

2. Summary of recommendations-------------------------------------- 20
   Operationalizing strategy to combat cybercrime----------------------------- 20

3. About ASSOCHAM------------------------------------------------ 22

4. Executive Team------------------------------------------------ 24

5. Our Offices------------------------------------------------------ 25
Perspective and learnings for India

Cyberspace has grown exponentially around the world. India too has witnessed a significant rise in internet activities. Such phenomenal growth in access to information and connectivity has on one hand empowered individuals and organization and on the other posed new challenges to government and citizens.

Making the cyber world safer is of primary interest to all stakeholders. Putting up deterrent measures against cybercrime is essential to national cybersecurity as well as for protecting critical infrastructure of the nation. Enforcing data security measures and creating proactive security monitoring capability are vital for an organization to maintain a lead over emerging threats and protect their financial, intellectual and customer-related information. Overall, we all agree that cybercrime is an increasing menace. However, no matter how many controls or tools businesses and individuals obtain; the government's role in providing a secure ecosystem can never be underplayed. A secure cyberspace and government's influence in keeping tabs on cybercrime have become important criteria for businesses to establish, operate and flourish in any region. The measures adopted for prevention, response and recovery form an integral part of the government's accountability; although it is a shared responsibility. At the regional and international level, governments need to take the lead in forging meaningful relationships. Global menace of cybercrime and threats originating from the digital world require dedicated resources and efforts. A slew of measures have been adopted by several countries around the globe for prevention, detection, investigation and speedier trial of cybercrimes. An overview of India's current cybersecurity initiatives and some of the leading practices adopted globally is presented below. While some nations have taken extreme measures based on their political orientation, others have successfully balanced their executive powers granted to such institutions and factors related to individual rights and privacy.

Further, as part of this document we factored seven key aspects, which may be important for building a strong foundation to counter cybercrimes.

With best regards,

(Rahul Rishi)
As the nation embarks to connect over 1.2 billion people and leapfrog into next generation infrastructure including smart cities, millions of people, devices and machines are getting hyper-connected across India every day. 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 lives of hundreds of millions of people, improve 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-government and improve crop yields in seconds can disrupt life as we know it. From critical communications network to power distribution to financial well-being of the nation depends on the robustness of the cyber network. Each day, there are growing reports of spread of malware, misinformation and systemic cyber-attacks. These malicious forces know no physical boundaries. This is a huge challenge and needs unprecedented collective action. Indeed, it is now a paramount national priority.

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

Intelligent tools to counter cyber and network threats will require convergence of Big Data, analytics and machine learning technologies. We are working with all our stakeholders to develop these tools and develop enabling policies to enhance cyber and network security. With that backdrop, ASSOCHAM is organizing the seventh edition of the Annual Cyber & Network Security Summit on 26 August 2015 at Hotel The Ashok in New Delhi. This will present a unique opportunity to have a contemporary dialogue among all key stakeholders – governments, industry, academia and civil society.

With best regards,

(Pratyush Kumar)
The growing use of ICT for administration and in other spheres of our daily life cannot be ignored. In the era of e-governance and e-commerce, a lack of common security standards can create havoc for the global trade in goods and services.

With the focus on creating and securing Digital India, the threat from cyber attacks and malware is not only apparent, but also very worrisome. There cannot be a single solution to counter such threats. We need a techno-legal “Harmonized Law” and cooperation among states, agencies and countries to address these challenges.

A good combination of law and technology must be established, and then an effort must be made to harmonize the laws of various countries keeping in mind the common security standards.

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 effective dealing with internal and external cybersecurity threats.

We are confident that the deliberations at the 7th Annual Summit on Cyber & Network Security - 2015, with the theme Securing the Digital India will provide more insights to the emerging cyber-related challenges and their appropriate solutions for further securing the cyberspace.

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

We convey our very best for the success of the 7th Annual Summit on Cyber & Network Security 2015.

With best regards,

(D. S. Rawat)
The risks of operating in the cyber world are reaching unprecedented levels as newer forms of threats and vulnerabilities continue to emerge. Such threats are becoming harder to predict as well as targeted in nature. With the ever-shrinking difference between the cyber and physical world, and the use of a large number of internet-connected devices, the threat actors are seemingly well-positioned to cause disruption to a nation’s government, businesses and citizens alike. As technology continues to offer numerous benefits to society, a number of divergent scenarios continue to stifle its widespread adoption and growth. Cybercrime has fast established itself as the “Achilles heel” of living in the cyber age. To prevent such misuse of information and communications technology (ICT) for criminal activities requires a coordinated effort involving the country’s government, businesses, residents as well as collaboration with international agencies.

The formulation of a national strategy and development of protection frameworks to support such strategies is essential for reducing the risks of cybercrime. Legal and institutional support, as well as capacity building of law enforcement agencies require cooperation of all stakeholders. However, the government remains imperative. Development of legislative mechanisms and criminal law provisions to tackle the menace of cybercrime, as well as ensuring that concerned agencies have the necessary training, tools and know-how to take on new age cybercrimes are other areas that the government must focus on.

The Digital India program¹ of the Government of India is leading a very important role in the economic, demographic and social transformation of the country. The goal of connectivity for all – leading to rapid expansion of digital fiber links connecting the nation; creation of digital identity – enabling every citizen to utilize services online; and financial inclusion – leading to operationalization of banking facility over mobiles for millions can only be met if there is a secure cyberspace to transact in. Overall, to counter the global menace of cybercrime and threats originating from the digital world, we require dedicated resources and efforts.

As part of this document, an analysis of the prevailing cyber ecosystem in India and the various measures undertaken by the Government to increase the trustworthiness of cyberspace, as well as in managing issues related with cybercrime is presented.

1. India: current cybercrime landscape and leading practices across globe

1.1 National level plan/strategy

The availability of a national strategy around cybersecurity demonstrates the government’s commitment in laying down objectives and goals to help ensure a secure cyberspace. Currently, as part of the 12th Five Year Plan² (2012-17), a strategic approach has been defined for cybersecurity initiatives. This plan focuses on the following key areas:

► Enabling legal framework
► Security policy, compliance and assurance
► Security research and development
► Security incident – early warning and response
► Security awareness, skill development and training
► Collaboration

¹http://www.digitalindia.gov.in/content/about-programme
²http://planningcommission.gov.in/plans/planrel/12thplan/pdf/12fyp_vol2.pdf
### DeitY’s objectives and major initiatives

<table>
<thead>
<tr>
<th>Primary objectives</th>
<th>Actions to secure cyberspace</th>
<th>Major initiatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>▶ Prevent cyber attacks against the country’s critical infrastructures</td>
<td>▶ Forensics and attack attribution</td>
<td>▶ Security policy, compliance and assurance</td>
</tr>
<tr>
<td>▶ Reduce national vulnerability to cyber attacks</td>
<td>▶ Protection of networks and systems critical to national security</td>
<td>▶ Security incident – early warning and response</td>
</tr>
<tr>
<td>▶ Minimize damage and recovery time from cyber attacks</td>
<td>▶ Early watch and warnings</td>
<td>▶ Security training – skills/competence development and end user awareness</td>
</tr>
<tr>
<td></td>
<td>▶ Protection against organized attacks capable of inflicting debilitating damage to the economy</td>
<td>▶ Security R&amp;D for securing the infrastructure, meeting the domain-specific needs and enabling technologies</td>
</tr>
<tr>
<td></td>
<td>▶ Research and technology development that will enable the critical infrastructure organizations to secure their IT sets</td>
<td>▶ Security – promotion and publicity infrastructure organizations to secure their IT sets</td>
</tr>
</tbody>
</table>

---

DeitY’s objectives and major initiatives
Taking lead from the Five Year Plan, the Department of Electronics and Information Technology (DeitY), India has also defined a cybersecurity strategy. DeitY states that the risks associated with current and anticipated vulnerabilities of, threats to, and attacks against the IT infrastructure provide the rationale for this strategy.

The primary objectives of DeitY’s cybersecurity strategy revolve around three primary objectives, which are supported by five actions and strategic initiatives.

The current cybersecurity strategy of DeitY mostly focuses on the areas as defined in the Five Year Plan. Although the plan covers most of the domains impacted by cyber security, the initiatives and road maps listed for each of the key areas are still at a very nascent level. They fall short of addressing a broad set of issues and challenges related with the complexity of cybercrime. Though a few agencies and bodies have been notified, there is much to be done to realize the objective of this strategy. India is yet to see an assurance mechanism to measure compliance with the government security policy. Cyber incident early warning systems and a coordinated response mechanism are yet to forge as a cohesive function. There are huge gaps in the level of trained cybersecurity professionals available in the country as compared to the overall needs, and R&D in cybersecurity is at dismal levels. There are gaps in the availability of proficient cyber experts within law enforcement agencies and the lack of appropriate implementation of the strategy means that a very few measures are in place to immobilize a larger set of cyber sleuths to counter the menace of cybercrime. The implementation of the cybersecurity strategy in India is still in its infancy. However, positive steps have been taken by the government, especially in wake of recent surge in adopting digital technology for governance and providing citizen-centric services. It is worth mentioning that currently only a few nations have successfully put into motion, strategic initiatives for cybersecurity. Some examples of leading practices followed by nations for successfully translating their cybersecurity strategy into on-ground initiatives are presented below.

Global leading practices

Countries, such as the United States of America (USA) and the United Kingdom (UK) have reached an advanced stage as far as the implementation of their cybersecurity strategy is concerned. Australia has formulated a national plan to combat cybercrime with a vision of safe and secure digital environment for all Australians. Canada’s cybersecurity strategy is focused on a plan for meeting cyber threat and help Canadians to be secure online.

While India is in the process of defining key initiatives with regard to cybersecurity, many mature countries have already implemented various key initiatives aimed at the improvement of critical infrastructure for cybersecurity and addressing cybercrime.

In addition to the existing mechanisms, a strategy needs to be documented, which states the vision, objective and approach for cybercrime prevention in India. A definite cybercrime prevention program may originate as a specific recommendation of such a document.

The strategy and execution of cybersecurity needs to be developed with clear vision for addressing challenges related with cybercrime in the short-term and mid-term with possible review mechanism to a long-term approach in this domain. The global practices from mature law enforcement organizations, such as the Federal Bureau of Investigation (FBI) and Interpol need to be leveraged and adopted as per their feasibility as part of the Indian cybercrime strategy.
1.2 Responsible agencies/departments

Cybercrime can only be effectively countered when there is a proper coordination and guidance available for various stakeholders, such as residents of a nation, industries as well as the local, state and central governments. To facilitate such cooperation as well as to give impetus and to govern the effective implementation of various initiatives, we need to have adequately tasked and staffed agencies working at various levels. In India, the Government had set up an Inter Departmental Information Security Task Force (ISTF) with the National Security Council as the nodal agency to coordinate all matters related with effective implementation of its cybersecurity strategy. Indian Computer Emergency Response Team (CERT-In) is the national nodal agency set up to respond to computer security incidents as and when they occur. Some of the activities undertaken by CERT-In toward cybersecurity include coordination of responses to security incidents and major events; issuance of advisories and timely advice regarding imminent threats; product vulnerabilities analysis; conduct trainings on specialized topics of cybersecurity; and development of security guidelines on major technology platforms. Another major initiative is by means of the creation of specialized teams at different departmental levels, such as:

- National Cyber Coordination Centre (NCCC)
- National Critical Information Infrastructure Protection Centre (NCIPC)
- Grid Security Expert System (GSES)
- National Counter Terrorism Center (NCTC)
- Cyber Command for Armed Forces
- Central Monitoring System (CMS)
- National Intelligence Grid (NATGRID)
- Network and Traffic Analysis System (NETRA)
- Crime and Criminal Tracking Network & Systems (CCTNS), in addition to the creation of sector-specific CERTs for power sector

The NCCC, with its first appointed chief is touted to play an integral role. This includes screening online threats and coordinate with the intelligence agencies to handle issues related to the national security by guarding against hackers and espionage, and tracking terrorist activity online. However, this appointment is yet to be followed up with any affirmative action. Moreover, the creation of a large number of agencies and bodies with similar mandates has led to deadlocks and jurisdiction issues, hampering the effective operation of these bodies. Another major challenge is the low involvement of the private industry in major government initiatives.

Addressing cybercrime does not merely imply that the government will need to task itself with all responsibilities and will be able to find answers in a silo. Victims of cybercrime, be it individuals or organizations, need to cooperate with law enforcement agencies for effective response. It is only through cooperation with each other that all stakeholders will be best-placed to understand the complexities involved and work together to build systematic and workable situations. India is yet to realize the full potential and benefits of a public-private partnership in the cybersecurity as well as cybercrime space.

Global leading practices

Some mature countries have leveraged partnership with private players and industry to equip them to counter the menace of cybercrime. For example, countries already have existing bodies or agencies, which are privately-led, but are supported by government agencies. For example in the USA, a privately-led Identity Ecosystem Steering Group (IDESG) has been established to support the National Strategy for Trusted Identities in Cyberspace (NSTIC). Similarly, the Australian Government has established the Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience. It is Australia’s primary national engagement mechanism for business-government information sharing and resilience building initiatives on critical infrastructure resilience. In Germany, the Federal

[^7]: http://www.nist.gov/nstic/
Office for Information Security (BSI)\(^9\) and the Federal Association for Information Technology, Telecommunications and New Media have launched a voluntary program called Alliance for Cybersecurity to inform and report on cyber incidents. The Cyber-security Information Sharing Partnership (CiSP)\(^10\) part of CERT UK is a joint initiative with private industry to share cyber threat and vulnerability information in order to increase the overall situational awareness of the cyber threat and therefore, reduce the impact on the UK businesses.

A dedicated national governing unit may be established in India, which will be the central agency for all state government cybercrime agencies to coordinate, integrate and share information related to cybercrime. Such a central agency will be responsible for driving all the cybercrime prevention initiatives, such as collaboration with private sectors, and training and awareness across the country.

### 1.3 Legal measures

According to various studies, ICT investments positively impact jobs, productivity, gross domestic product (GDP) growth and innovation. New ICTs, such as mobile communications and high-speed internet, in particular, are changing the way organizations do business, transforming public service delivery and democratizing innovation. New organizations are emerging, even as existing businesses work to gain the required agility to compete in today’s increasingly complex market landscape. Recently, there have been reports of an alarming number of incidents of both state and non-state actors using internet for reprehensible acts including identity theft, phishing, snooping, and denial of service; cyber-terrorism; and inducing threats for undermining the structures and systems of nations. While digital technologies are playing a major role in business transformation, the threat from cybercrime has emerged as one of the biggest challenges for governments and organizations worldwide. Nations needs to focus on laws related to the use of ICT, protection for intellectual property and access to digital content, among other parameters.

Cybercriminals can gain access to financial data, compromise intellectual property of companies, tap sensitive national data and steal government records. These actions could compromise national security and interests. India has struggled to cope with the implementation of its cybercrime laws. The country has approved amendments\(^11\) to its IT Act, 2000; however, technology has grown leaps and bounds complicating legal response and calls for a review. The IT Act penalizes various cybercrimes and provides punishments (imprisonment terms up to 10 years and fines up to INR1 crore, in some cases).

The IT (Amendment) Act, 2008\(^12\), has included the following:

- Electronic signatures
- Corporate responsibility
- Definitions of important terms, such as intermediaries and communication devices
- Legal validity of electronic documents
- Role of adjudicating officers
- Requirements on data retention

---

\(^9\)https://www.bsi.bund.de/EN/Home/home_node.html
\(^10\)https://www.cert.gov.uk/cisp/
Some of the cybercrimes identified and covered by the IT Act includes:

- Hacking
- Data theft
- Spreading malicious content/virus
- Identity theft
- Email spoofing

The amendment introduced in 2008 Act does not really bring about much change with respect to encryption, except for expanding the scope of the government's power to order decryption. While earlier, under section 69, the Controller had powers to order decryption for certain purposes and order 'subscribers' to aid in doing so (with a sentence of up to seven years upon non-compliance). Now, the government may even call upon intermediaries to help it with decryption (section 69 (3)). Additionally, section 118 of the Indian Penal Code has been amended to recognize the use of encryption as a possible means of concealment of a 'design to commit [an] offense punishable with death or imprisonment for life'.

While such legal mechanisms are being developed, companies in India will need to increase investments to safeguard themselves against cybercrime. One of the key impacts is the increasing cost to recover from cyber fraudulence or data breaches. Other negative fallouts of cybercrime to a business include damage to brand and other reputational losses, and harm to customer relations and retention.

Global leading practices

Some countries, such as the USA follows a sectoral approach that consists of mixed legislation and regulations, and self-regulations. Data is grouped in several classes on the basis of their utility in the USA. Hence, a different law structure is followed for each class of data. Additionally, as compared with many other countries, such as the USA and the UK, there is a lack of actual framework in the IT Act in India. The European Union has declared a list of countries having adequate legal provisions to deal with cyber laws. The list includes Argentina, Canada, Switzerland, New Zealand and the USA. However, India still needs to get enrolled in this white list, but it cannot, unless it has a proper and adequate legislation around cyber law.

Some improvement in the IT (Amendment) Act 2008, as compared with legislations of some other countries, and associated recommendations are given below:

- The IT (Amendment) Act 2008, in its current form, primarily deals with extraction, retention, communication and destroying of data. It needs to be updated and have a wider scope to include a legal framework for cyber laws.
- The IT (Amendment) Act 2008 Act does not cover majority of the crimes committed through mobiles. This needs to be rectified.
- A holistic data protection regime needs to be incorporated in the law to make it more effective.
- A right balance needs to be found between blocking the privacy of the citizens and monitoring the crime levels. India has seen some region-specific violence; the reason was that improper information went viral on social networking websites. However, the recent scrapping of section 66 A does not allow the intermediaries to bring down such hatred information. The act needs to be expanded further and there is a strong need to introduce more clarity in terms of responsibilities of intermediaries and encryption mechanisms.
1.4 Training and awareness

As the numbers of internet users are increasing day by day, high computing devices are now available with almost every individual providing access to entire cyber world. Although, technology uptake by individuals is very high, they fail to understand the underlying and inherent cyber risks associated with such technology and become easy targets for cybercriminals. It is important to spread awareness on cybercrime prevention since the cybercriminals are constantly inventing new ways to attack and are in search of potential victims. In fact, some of the most recent attacks on critical infrastructure of a few countries were perpetuated and successfully executed due to the low awareness level of most users, through phishing and social engineering methods.

Currently in India, looking at the growing importance for information security, DeitY has identified information security awareness as a critical area to focus on. Information Security Education and Awareness (ISEA) Project was formulated and launched in 2005 for five years. One of the activities under this program was to generate information security awareness to children, home users and non-IT professionals in a planned manner. The Department of Electronics and Information Technology under the Indian Ministry of Communications and Information Technology has assigned the responsibility of executing this project to the Centre for Development of Advanced Computing (C-DAC), Hyderabad. As part of the initiative, internet security awareness materials in the form of presentations, posters, cartoons, guide books, security tools and parental controls were designed for children. As part of this initiative, web portal ‘www.infosecawareness.in’ was also launched. Government has formulated investigation manuals with procedures for search, seizure analysis and presentation of digital evidence in courts. The manuals were circulated to law enforcement agencies in all states of the country.

1http://www.isea.gov.in/sea/index.jsp
The Government should provide well-defined citizen awareness programs aimed at preventing cybercrime as a proactive mitigation. This has to be achieved through multiple media, such as print, radio and web to ensure faster and maximum reachability with local and national languages. Cybercrime awareness shall be introduced in academics in the early stages of education as a mandate for all the state and central, and public and private schools. Mechanisms shall be established for independent monitoring of awareness program at regular intervals to evaluate the number of people/regions covered. Awareness material shall be updated regularly to cover up-to-date information.

The Australian Government has taken multiple initiatives for raising cybersecurity awareness based on age group, such as Cybersmart, Stay Smart Online and Cybersecurity builder, to educate children and other public about cybersecurity.

The UK has also initiated a national program, Get Safe Online with the objective of raising awareness about cybersecurity to general public. In addition, the government has also published advisory on cybersecurity for the private sector.

Global leading practices

Many mature countries, such as the USA has taken multiple initiatives to train and raise the public awareness on cybersecurity, as well as for law enforcement agencies, such as:

► National Cyber Security Awareness Month (under the brand of Stop.Think.Connect.)
► National Initiative for Cybersecurity Education (NICE)
► National Cybersecurity Education Council (NCEC)
► Cybersecurity Education and Training Assistance Program (CETAP)
► National Centers of Academic Excellence (CAEs) that provide students valuable technical skills in various disciplines of information assurance

Although, a project was launched for increasing the awareness among general public, sustenance of the program is not happening on a continuous basis. There is no dedicated agency to monitor the status of these awareness programs and their coverage. Also, there is no national help line/call center for common public that can guide them about dealing with cybercrime and reporting mechanisms.
1.5 Cybercrime reporting mechanism

Cybercrime, like any other crime, should be reported to appropriate law enforcement authorities depending on the scope of the crime. Since cybercrime is borderless, it is important that each and every citizen should be able to report cybercrime from any corner of the country.

The existing systems in India for reporting cybercrime involves registering complaints with the local police stations or cybercrime cells. Many of the Indian states have setup cybercrime cells, which monitor such crimes.

In several instances, victims may not be able to reach the police station to report a cybercrime due to several reasons, such as remote location, unawareness of exact place to report and privacy issues. This may results in many cybercrime cases being unreported.

There is no centralized online cybercrime reporting mechanism, which provides victims of cybercrime, a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations.

Also for law enforcement agencies at the national, state, and local level, there is no central referral mechanism for complaints involving cybercrime.

Global leading practices

Many tech-savvy countries such as in the USA, complaints can be filed through an online portal – Internet Crime Complaint Center (IC3). IC3 was established as a partnership between the FBI and the National White Collar Crime Center (NW3C) to receive internet-related criminal complaints and to further research, develop, and refer the criminal complaints to national, state, local, or international law enforcement and/or regulatory agencies for any investigation.

The UK Government has the provision of reporting inappropriate and offensive content in the website of Child Exploitation and Online Protection Centre (CEOP) for children and other cybercrime can be reported in the website of the Internet Watch Foundation. The UK Government has provided a dedicated helpline number for reporting cybercrime.

Cybercrime in Germany can be reported in the website of the Voluntary Self-Monitoring of Multimedia and Service Providers. New Zealand National Cyber Security Centre (NCSC) provides a dedicated number and website for reporting of cybercrime centrally.

Currently, India does not have the provision for a central online reporting for cybercrime and maintain a central repository of all the types of crimes reported across the country.

In order to increase the rate of reporting cybercrime, it is important to have provisions for online reporting of the crime. Using this system, an online cybercrime complaint can be made by the victims of cybercrime. They will gain access to a convenient and easy-to-use reporting mechanism that alerts law enforcement authorities of suspected criminal or civil violations. Also, it will provide a central repository for reference to law enforcement and regulatory agencies at the national, state and local level.

Maintaining centralized cybercriminal database

A centralized database of cybercriminals should be maintained so that the criminals released from jails may be monitored. Such checks will discourage cybercriminals from engaging in spurious activities in cyberspace. Many countries, such as the USA and Australia have maintained a central repository of cybercrimials.
1.6 International collaboration to thwart cybercrime

We all know that the cyber world transcends all physical barriers. Being transnational in nature, it is but obvious that nations across the globe need to strengthen their cooperation and form alliances as well as ensure that their legal, technical and institutional measures; structures are created; and work in coherence. Therefore, it is necessary that nations are able to reach consensus and work toward establishing a framework of international cooperation.

India, being one of the world’s largest IT players and with the experience of working with almost all countries, is yet to form any substantial partnerships on tackling cybercrime. The increasing use of social media, adoption of cloud services and uptake of technology sourced from global providers correspond to an increase in the threat landscape, which is clearly not the best tackled in isolation. While attacks on cyber infrastructure and threats from global cybercrime syndicates are surmounting, the response has been inadequate since data critical for investigation may be parked in servers beyond physical boundaries, or the actual perpetrator of the crime may be beyond the Indian jurisdiction. Although, a few treaties and measures exist; a holistic approach defining legal measures, technical measures and organizational capabilities is yet to assume central importance for India in its quest to contribute to the global fight against cybercrime.

Though the IT Act, 2008\(^1\) qualifies an attack on a computer, computer system or network located in India, from any entity or person outside India, as a crime; it lacks the necessary jurisdiction and control over authorities and law enforcement agencies where the criminals may reside, thus making it extremely difficult to gain access to information for the purpose of any investigation, prosecution and consecutive extradition on a foreign national. Although, Mutual Legal Assistance Treaties\(^2\) (MLATs) have been operationalized with over 34 countries and India along with other South Asian Association for Regional Cooperation (SAARC) countries has signed a Convention on Mutual Assistance in Criminal Matters in 2008, the efficacy of these treaties has always been in question. MLATs plays an important role in combating transnational organized crime and other serious offences, such as drug trafficking and money laundering. Even with an existing treaty, the necessary capability is not available with the law enforcement agencies to operationalize such measures when the need arises.

However, India remains a non-signatory on the Budapest Convention, which is the international treaty seeking to address cybercrime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. It is specifically designed to facilitate international cooperation to fight cybercrime. This assumes greater significance, since India has not been part of globally coordinated projects, such as Global Action on Cybercrime (GLACY), an initiative of the European Union and Council of Europe aimed at supporting countries with the implementation of Budapest Convention.

Lack of collaboration with international agencies leads to delay in investigation activities in case cybercrime involves a criminal from a different country. Additionally, India has to forego the benefits associated with forging international alliances through transfer of the best practices followed by countries for combating cybercrime. Global partnerships are no longer just an advantage, they have become necessary.

**Global leading practices**

Many international organizations are collaborating and making efforts to fight against cybercrime like the UN General Assembly adopted resolution dealing with computer crime legislation, combating the criminal misuse of information technology. The International Telecommunication Union (ITU), as a specialized agency within the United Nations, plays a leading role in the standardization and development of telecommunications and cybersecurity issues. The European Cybercrime Centre (EC3) has entered into partnerships with

---


\(^2\)[http://mha.nic.in/policy_planing_division]
It will be beneficial to have collaborations with International Cyber Security Protection Alliance, such as the Australian Cyber Security Centre (ACSC), National Crime Agency’s National Cyber Crime Unit (NCCU) and the UK’s CEOP. This will help in not only adopting the best practices by other countries for prevention of cybercrime, but also in increasing the capability, knowledge, training, skills, capacity and expertise of cybersecurity task forces. Additionally, it will help to reduce the harm caused to businesses, customers and citizens due to international cyberattacks.

India should be actively engaged as part of the international cybercrime associations centered on Asia/Europe and America to seek help and contribute for international cybercrime issues.

Budapest Convention on Cybercrime[^16], which is the first international treaty on cybercrime dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security, was signed by more than 45 countries.

[^16]: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

Canadian Cyber Incident Response Centre (CCIRC) works closely with its international counterparts such as the US-CERT, CERT-UK and CERT Australia.
1.7 Capacity building for strong cybersecurity

The cyberspace is a critical resource and possibly the greatest virtual environment ever created. Advancement in technology has connected people, communities and businesses around the world. The rapid expansion of the cyber world also brings with it a surge of malicious activities. Capacity building is one of the most important aspects to strengthen cybersecurity. Some of the key Initiatives taken by the Government of India for capacity building are as follows:17

Manpower development

Cybersecurity training facilities have been setup to provide training for law enforcement agencies and facilitate cybercrime investigation. Following initiatives have been taken for manpower development:

► The Ministry of Home Affairs has issued an advisory on cybercrime to the state governments and the union territory administrations. The state governments have been advised to build adequate technical capacity in handling cybercrime, including technical infrastructure, cyber police stations and trained manpower for detection, registration, investigation and prosecution of cybercrime. Also, action has been taken to setup a national center of excellence, exclusively devoted to render cyber forensic services and to act as a national research and training center on cyber forensics.

► Many initiatives were taken by government organizations, such as CERT-In and CDAC were providing basic and advanced training to police officers, judiciary officers and other law enforcement agencies on the procedures and methodology of collecting, analyzing and presenting digital evidences. Cybercrime investigation manuals were circulated to all state police stations.

► Further, a cyber forensics training lab was set up at the Training Academy of Central Bureau of Investigation (CBI) to impart basic and advanced training in cyber forensics and investigation of cybercrimes to police officers associated with the CBI. In addition, the Government has setup cyber forensic training and investigation laboratories in the states of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur, and Jammu and Kashmir for training of law enforcement and judiciary in these states.

Cybercrime cell and cyber forensics lab

Ministry of Home Affairs is supporting the establishment of Cyber Crime Police Station (CCPS) and Cyber Crime Investigations and Forensic Training Facilities (CCIFTF) in each state/union territory of India under Police Modernization Scheme. Also to combat cybercrime, CBI has setup multiple centers18 for cybercrime research and investigation, such as Cyber Crimes Research and Development Unit (CCRDU), Cyber Crime Investigation Cell (CCIC), Cyber Forensics Laboratory and Network Monitoring Centre.

R&D

R&D is an essential component of capacity building measures due to various reasons, such as creation of knowledge and expertise to face new and emerging security challenges, produce cost-effective and advanced security environment. Currently, DeitY has set up a sub-group on cybersecurity for 12th Five Year Plan on Information Technology Sector, consisting of various experts/representatives from academic and R&D organizations, industry and user agencies on various issues related to cyber security R&D, and also has identified the key priorities for R&D.

Although initiatives have been taken to train and educate law enforcement officers about cybercrime, we lack sufficient skills to understand the technology evolution, and associated threats and vulnerabilities, which may be exploited.

Further, there is also a lack of capability to understand the psychological behavior of a cybercriminal. This is an important area of development since cybercriminals constantly look for innovative methods to exploit potential victim thorough channels, such as social engineering, sentiment analysis and stalking.

Lack of awareness and poor knowledge on handling digital evidence ceased from a crime scene leads to greater challenges

17http://164.100.47.134/isscommittee/Information%20Technology/15_Information_Technology_52.pdf
18http://cbi.nic.in/aboutus/manuals/
for a law enforcement officer than any skill issue. An officer re-designated to investigate cybercrime may unknowingly contaminate the digital evidence or store it in conditions, which may lead to the destruction of an evidence. Additionally, in order to identify the modus operandi of the criminal, it will be essential to understand the psychology of the cybercriminal rather than just relying on tools and technology.

Also, current tools/technologies are not sufficient enough to address the evolving cybercrime issues. This situation arises because of the lack of R&D in cybercrime domains.

**Global leading practices**

Many international organizations, such as the Council of Europe, the UN Commission for Crime Prevention and Criminal Justice have focused on capacity building as an effective way to address the challenges of cybercrime. They have agreed on policies for the member countries and action to share information for capacity building programs.

Germany had recognized national or sector-specific educational and professional training program for manpower development by promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

The U.S. Department of Defense (DOD) has established the Defense Industrial Base (DIB) Cybersecurity/Information Assurance (CS/IA) Program that aims to provide cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

The Cybersecurity Division (CSD) of the U.S. Department of Homeland Security provides information resources – standards, frameworks, tools, and technologies to enable seamless and secure interactions among homeland security stakeholders and leads the government’s charge in funding cybersecurity R&D.

Skilled law enforcement personnel are the need of the hour, considering the highly technical and advanced nature of cybercrime being reported. To gear up to speed in containing and preventing cybercrime, there is a need to engage more cybercrime investigation professionals. Such personnel may be deployed at state level with access to dedicated laboratories for analysis at each state. Such teams also need to be part of the police team investigating cybercrimes. There should be a special recruitment for personnel to man cyber cells at every police station.

There is a need to increase the number of cybercrime cells and laboratories in the states and provide requisite manpower, training and infrastructure to them. Initiatives to setup the cybercrime cells and laboratories in states where these do not exist, and also upgrade and strengthen the existing cybercrime cells is required to cope up with the rapid cybercrimes. There is a need to establish a centralized repository for cybersecurity standards, best practices and guidelines, which can be used by law enforcement agency for preventing and investigating cybercrime.
2. Summary of leading global practices

Once a national framework and strategy for cybersecurity are formulated, it is imperative that robust mechanisms for swift implementation are created. Protection for cybercrime does not merely entail creating institutional mechanisms and agencies equipped with the latest forensic and investigation tools. It also depends on the ability of the end user to safeguard himself against malicious online content, for which the government may launch programs to increase public awareness. Similarly, the availability of technical systems, which may protect computing resources and skilled manpower to design, build, operate and maintain such technical systems helps in reducing risks of cybercrime. This may require extensive R&D, creation of an ecosystem for organizations which possess such capability to thrive. Thus, the fight against cybercrime can only be successful, if there is traction regarding measures suggested in the national cybersecurity strategy.

While there may be several approaches to building a cyber secure environment, it is worthwhile to refer to the ITU National Cybersecurity Guide\(^\text{19}\), as it presents a view of elements contributing to the development of a holistic, strategy-led cybersecurity program.

<table>
<thead>
<tr>
<th>Government body</th>
<th>Cybersecurity Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Cybersecurity Accountability</td>
<td>Dedicated Ministry accountable for devising a national strategy and fostering local, national and global cross-sector cooperation.</td>
</tr>
<tr>
<td>National Cybersecurity Coordinator</td>
<td>Department or individual who oversees cybersecurity activities across the country</td>
</tr>
<tr>
<td>National Cybersecurity Center Point</td>
<td>A multi-agency center, which serves as a focal point for all activities dealing with the protection of a nation’s cyberspace against all types of cyber threats.</td>
</tr>
<tr>
<td>Legal measures</td>
<td>Review of cyber laws and, if necessary, amend the existing law, create new procedures, and policy to deter, respond to and prosecute cybercrime</td>
</tr>
<tr>
<td>National cybersecurity framework</td>
<td>Framework that defines minimum or mandatory security requirements on issues, such as risk management and compliance</td>
</tr>
<tr>
<td>Cybercrime reporting and analysis</td>
<td>Analysis of cyber threat trends, coordinates response and disseminates information to all relevant stakeholders</td>
</tr>
<tr>
<td>Cybersecurity awareness and education</td>
<td>A national program to raise awareness about cyber threats on a continuous basis</td>
</tr>
<tr>
<td>Capacity building</td>
<td>A program to train cybersecurity professionals</td>
</tr>
<tr>
<td>International cooperation</td>
<td>Adequate infrastructure for cybercrime prevention and investigation</td>
</tr>
</tbody>
</table>

\(^{19}\text{http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf}\)
Operationalizing strategy to combat cybercrime

To positively impact the cybersecurity ecosystem and to combat cybercrime, it is imperative that efforts and resources are dedicated to operationalize a nation’s cybersecurity strategy. If such initiatives are driven from the highest level of the government, it ensures that all stakeholders are interested and engaged in contributing to the success of any initiatives or programs. Such commitment, though it is an important enabler, is not sufficient to guarantee the success of any initiative or program. Monitoring and review mechanisms are essential to analyze and assess progress as well as consider measures for re-calibration and course correction as may be required. It is important to define milestones and operationalize the strategy as per the desired impact of initiatives, which are being undertaken.

A sample road map basis impact of initiatives is presented below. While several initiatives may commence in parallel, the graph presents a view of their impact on the overall ecosystem for combating cybercrime.

Cybersecurity road map, based on period of impact

<table>
<thead>
<tr>
<th>Near - Term</th>
<th>Mid - Term</th>
<th>Long - Term</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cybersecurity Strategy</strong></td>
<td><strong>Legal Measures</strong></td>
<td><strong>International Cooperation</strong></td>
</tr>
<tr>
<td>- Define vision and objectives for two years and five years</td>
<td>- Review of IT act and, if necessary, amend the existing law</td>
<td>- Collaborations with International Cyber Security Protection Alliance.</td>
</tr>
<tr>
<td>- Define action plan to achieve cybersecurity strategy</td>
<td>- Create new procedures, and policy to defer, respond to and prosecute cybercrime</td>
<td>- Active participation in International Cybercrime associations</td>
</tr>
<tr>
<td><strong>Cybersecurity Capacity Building</strong></td>
<td><strong>Advance tools and technology</strong></td>
<td></td>
</tr>
<tr>
<td>- Training on cybercrime and digital evidence</td>
<td></td>
<td>- Collaborations with international cybersecurity protection alliance</td>
</tr>
<tr>
<td>- Increase number of cybercrime cell</td>
<td></td>
<td>- Active participation in international cybercrime associations</td>
</tr>
<tr>
<td>- Advance Forensics labs</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>National Agency for Cybersecurity</strong></td>
<td><strong>Cybersecurity reporting mechanism</strong></td>
<td></td>
</tr>
<tr>
<td>- Formation of national level Cybercrime Working Group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Defining objectives and action plans for National Cybercrime Working Group</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Training and Awareness</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>R&amp;D</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ASSOCHAM initiated its endeavour of value creation for Indian industry in 1920. Having in its fold more than 400 Chambers and Trade Associations, and serving more than 4,50,000 members from all over India. It has witnessed upswings as well as upheavals of Indian Economy, and contributed significantly by playing a catalytic role in shaping up the Trade, Commerce and Industrial environment of the country.

Today, ASSOCHAM has emerged as the fountainhead of Knowledge for Indian industry, which is all set to redefine the dynamics of growth and development in the technology driven cyber age of ‘Knowledge Based Economy’.

ASSOCHAM is seen as a forceful, proactive, forward looking institution equipping itself to meet the aspirations of corporate India in the new world of business. ASSOCHAM is working towards creating a conducive environment of India business to compete globally.

ASSOCHAM derives its strength from its Promoter Chambers and other Industry/Regional Chambers/Associations spread all over the country.

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

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

**Members - Our Strength**
ASSOCHAM represents the interests of more than 4,50,000 direct and indirect members across the country. Through its heterogeneous membership, ASSOCHAM combines the entrepreneurial spirit and business acumen of owners with management skills and expertise of professionals to set itself apart as 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 field of Corporate Social Responsibility, Environment & Safety, HR & Labour Affairs, Corporate Governance, Information...

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

ASSOCHAM derives its strengths from the following Promoter Chambers: Bombay Chamber of Commerce & Industry, Mumbai; Cochin Chambers of Commerce & Industry, Cochin; Indian Merchant’s Chamber, Mumbai; The Madras Chamber of Commerce and Industry, Chennai; PHD Chamber of Commerce and Industry, New Delhi 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

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 EY

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

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

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

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

© 2015 Ernst & Young LLP. Published in India. All Rights Reserved.

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

RB