Perry4Law
An Exclusive Techno-Legal Corporate, IP & ICT Law Firm

New Delhi, India

Cyber Security Trends And Developments In India 2013

The Cyber Law Trends and Developments of India 2013 (PDF) has already been covered by Perry4Law and Perry4Law's Techno Legal Base (PTLB). In this research work we are covering the Cyber Security Trends and Developments in India 2013.

(1) National Cyber Security Policy India: Cyber Security in India has been ignored for long. However, Indian Government realised that this is a crucial field and it needs a clear Cyber Security Policy. The National Cyber Security Policy of India 2013 (NCSP 2013) was drafted keeping this requirement in mind. It is a good Policy on many counts but it also failed to address many crucial aspects as well. For instance, the Policy has failed to protect Privacy Rights in India. Nevertheless, this is a good step in the right direction and it must be updated and improved as the time passes

(2) National Security Policy Of India: National Security of India is facing many challenges these days that are mainly attributable to the use and abuse of Information and Communication Technology (ICT). A National Security Policy of India is urgently needed that must have the Cyber Security Policy as an essential element. Presently this is not the case but we hope the same would be achieved very soon by the Indian Government.

(3) National Telecom Security Policy Of India: There is no implementable National Telecom Security Policy of India as on date. However, it may be drafted very soon by the Indian Government. As of now the Telecom Service Providers of India are openly flouting the Laws of India. They are not following the Cyber Law Due Diligence in India. For instance, Airtel and Tata Teleservices Limited are violating Cyber Law of India in general and Internet Intermediary Rules of India in particular. These violations must be punished by Department of Telecommunication (DoT) and Telecom Regulatory Authority of India (TRAI). Even the Defence Research and Development Organisation (DRDO) has communicated to the DoT that the proposed National Telecom Security Policy should have a framework to penalise Telecom Service Providers if they fail to abide by the norms.

(4) Imported Software And Telecom Equipments Security: Cyber Security of imported Software and Telecom Products was a major cause of concern for India. For instance, Huawei and ZTE have already faced Telecom Security Issues in India. Similarly, India is also considering making the Norms for import of Telecom Equipments in India more stringent. The Security Agencies of India have gone to the extent of even suggesting for the developing indigenously manufactured Cyber Security Software. Although the testing of Imported Software and Hardware for embedded Malware has been postponed till 1st April 2014 by India yet this issue would resurface in the year 2014. Even a Telecom Security Directorate of India has been proposed by Indian Government.

(5) Cyber Security Of E-Governance: Cyber Security of E-Governance Services in India is still not upto the mark. The Cyber Security in India must be improved so That Public Services can be better delivered through the mode of E-Governance and Mobile Governance. Similarly, Cyber Security Legal Practice must be encouraged and developed in India so that Cyber Crimes and Cyber Security related breaches can be properly prosecuted.

(6) E-Mail Policy Of India: There has been an increase in the use of Private E-Mails for committing Cyber Crimes in India and world wide. For instance, E-Mail Service Providers like G-mail are abetting and encouraging commission of Cyber Crimes. E-Mail Service Providers like G-Mail, Yahoo, Hotmail, etc are also facilitating violating the provisions of Public Records Act, 1993 wherever public Records are involved and they must be banned in India. Realising the seriousness of the situation, Delhi High Court is analysing E-Mail Policy of India and complaint mechanism to Facebook. The Delhi High Court has also directed Central Government to Issue Notification regarding Electronic Signature under Information Technology Act 2000. An advisory by Maharashtra Government to use official E-Mails has already been issued. Even the E-Mail Policy of India has been proposed by Indian Government.

(7) Cyber Security Of Private Banks In India: Cyber Security of Banks in India is still not taken seriously. Banks are not interested in ensuring Cyber Security of electronic transactions. The Recommendations of Reserve Bank of India (RBI) to ensure Cyber Security, appointment of Chief Information Officers (CIOs), establishing a Steering Committee at board level, etc has remained unfulfilled. Even RBI has warned banks for inadequate Cyber Security.

If the online business or transaction pertains to Banking Industry, especially online transfer and receiving of money, the applicable provisions can include the Internet Banking Guidelines, Mobile Banking Security Practices, e-Commerce Regulations and Compliances, Risk Management for Card Present Transactions, etc.

(8) Mobile Payment Cyber Security: Mobile Security in India is still a serious concern in India. The truth is that India is Not Ready for Mobile Governance as on date. Mobile Banking Cyber Security in India is still missing and the same must be established on a priority basis. Incidences of ATM Frauds, Credit Card Frauds, Phishing, RTGS Frauds, Internet Banking Frauds, etc have increased significantly in India. Malware targeting mobiles specifically have also raised the threat level further. On top of it we have poor adoption cyber security practices and policies by banks of India. In short, the Online Banking System of India is Not Cyber Secure and Mobile Payments Cyber Security in India is needed especially when the RBI is suggesting use of SMS Based Funds Transfer in India.

(9) Cyber Security Capabilities: Incidences of Cyber Crimes, Cyber Attacks, Cyber Security Incidences, Cyber Warfare, Cyber Terrorism, Cyber Espionage, etc are some of the problems that are peculiar to the contemporary times. These threats are intimidating the National Security of India by striking at the Financial, Economic, Social and Political Environment of India. Offensive and Defensive Cyber Security Capabilities of India is need of the hour. Even the National Cyber Security Policy of India 2013 (NCSP 2013) (PDF) recognised this fact. Techno Legal Skills Development in India is need of the hour and India must stress more upon Online Skills Development and E-Learning Methods to fill this skills gap.

(10) Cyber Security Legal Practice: Cyber Security Legal Practice is the emerging Global Trend. Naturally, Cyber Security Legal Practice in India is still maturing. More and more Law Firms and Lawyers need to take up Cyber Security as a Legal Practice in India.

(11) Cyber Security Awareness In India: Cyber Security Awareness in India is required to be enhanced. Keeping this in mind, the Cyber Security Awareness Brochures were mooted in India by Indian Government. Now Computer Hardware Providers in India are required to mandatorily provide Cyber Security Awareness Brochures along with their Products.

(12) Cyber Security Disclosure Norms In India: The Cyber Security Infrastructure in India is struggling hard to catch up the Malware ridden Internet and growing Cyber Attacks against India. As there is no requirement to inform about a Cyber Security Breach and Cyber Security Incidence, no private company or institution in India is reporting such crucial Cyber Security Incidences. To tackle this situation, the Indian Government is planning a Legislation Mandating Strict Cyber Security Disclosure Norms in India. This is a good step in the right direction provided the Indian Government actually implements what it has suggested.

There are many more aspects that we wish to discuss these Trends but due to the limited scope of this work, we are restraining from doing so. Perry4Law and PTLB hope that our readers would find this Trend useful.