

CYBER LAW OBJECTIVES

http://www.tutorialspoint.com/information_security_cyber_law/cyber_law_objectives.htm

Copyright © tutorialspoint.com

The recent Edward Snowden revelations on the US surveillance program PRISM have demonstrated how a legal entity network and computer system outside a particular jurisdiction is subject to surveillance without the knowledge of such legal entities. Cyber cases related to interception and snooping are increasing at an alarming rate. To curb such crimes, cyber laws are being amended quite regularly.

Emerging Trends of Cyber Law

Reports reveal that upcoming years will experience more cyber-attacks. So organizations are advised to strengthen their data supply chains with better inspection methods.

Some of the emerging trends of cyber law are listed below –

- Stringent regulatory rules are put in place by many countries to prevent unauthorized access to networks. Such acts are declared as penal offences.
- Stakeholders of the mobile companies will call upon the governments of the world to reinforce cyber-legal systems and administrations to regulate the emerging mobile threats and crimes.
- The growing awareness on privacy is another upcoming trend. Google's chief internet expert Vint Cerf has stated that *privacy may actually be an anomaly*.
- **Cloud computing** is another major growing trend. With more advancements in the technology, huge volumes of data will flow into the cloud which is not completely immune to cyber-crimes.
- The growth of **Bitcoins** and other virtual currency is yet another trend to watch out for. Bitcoin crimes are likely to multiply in the near future.
- The arrival and acceptance of data analytics, which is another major trend to be followed, requires that appropriate attention is given to issues concerning **Big Data**.

Create Awareness

While the U.S. government has declared October as the National Cybersecurity Awareness month, India is following the trend to implement some stringent awareness scheme for the general public.

The general public is partially aware of the crimes related to **virus transfer**. However, they are unaware of the bigger picture of the threats that could affect their cyber-lives. There is a huge lack of knowledge on e-commerce and online banking cyber-crimes among most of the internet users.

Be vigilant and follow the tips given below while you participate in online activities –

- Filter the visibility of personal information in social sites.
- Do not keep the "remember password" button active for any email address and passwords
- Make sure your online banking platform is secure.
- Keep a watchful eye while shopping online.
- Do not save passwords on mobile devices.
- Secure the login details for mobile devices and computers, etc.

Areas of Development

The "Cyberlaw Trends in India 2013" and "Cyber law Developments in India in 2014" are two prominent and trustworthy cyber-law related research works provided by Perry4Law Organization

P4LO for the years 2013 and 2014.

There are some grave cyber law related issues that deserve immediate consideration by the government of India. The issues were put forward by the Indian cyber law roundup of 2014 provided by P4LO and Cyber Crimes Investigation Centre of India *CCICI*. Following are some major issues –

- A better cyber law and effective cyber-crimes prevention strategy
- Cyber-crimes investigation training requirements
- Formulation of dedicated encryption laws
- Legal adoption of cloud computing
- Formulation and implementation of e-mail policy
- Legal issues of online payments
- Legality of online gambling and online pharmacies
- Legality of Bitcoins
- Framework for blocking websites
- Regulation of mobile applications

With the formation of cyber-law compulsions, the obligation of banks for cyber-thefts and cyber-crimes would considerably increase in the near future. Indian banks would require to keep a dedicated team of cyber law experts or seek help of external experts in this regard.

The transactions of cyber-insurance should be increased by the Indian insurance sector as a consequence of the increasing cyber-attacks and cyber-crimes.

International Network on Cybersecurity

To create an international network on cybersecurity, a conference was held in March 2014 in New Delhi, India.

The objectives set in the International Conference on Cyberlaw & Cybercrime are as follows –

- To recognize the developing trends in Cyberlaw and the legislation impacting cyberspace in the current situation.
- To generate better awareness to battle the latest kinds of cybercrimes impacting all investors in the digital and mobile network.
- To recognize the areas for stakeholders of digital and mobile network where Cyberlaw needs to be further evolved.
- To work in the direction of creating an international network of cybercrimes. Legal authorities could then be a significant voice in the further expansion of cyber-crimes and cyber law legislations throughout the globe.

Loading [MathJax]/jax/output/HTML-CSS/fonts/TeX/fontdata.js