International Journal of Academic Research
ISSN: 2348-7666 : Vol.2, Issue-4(6), October-December, 2015
Impact Factor : 1.855

Information security awareness & Youth- new legislative Implications

Dr. Mutharaju S . H. Assistant Professor & H.O.D. Department of Political Science, Government First Grade College, KANAKAPURA, Ramanagara District-562117, Karnataka state

Abstract: Information security awareness is a new mode of creating awareness among users especially youth. There is need to create an awareness for youth about crimes through new technology its preventive measures & the political support through legislations against cybercrime. Student who uses technology very often become addicted to internet & there are nearly 250 million internet users in India. Despite legislative support internet crimes are increasing & youth have been subjects to several types of crimes as they are being used as a medium of spreading cybercrime. The vulnerable youth are a prey to such activities. This paper addresses the issues of Cyber Crime, legislation & legal support against crime & considers involving youth against cyber related anti-social activities.

Key words: cyber related crimes cyber laws, legal support, youth, need for strong cyber legislations.

Introduction: The expansion of internet technology is causing a lot of problems leading to cybercrime. The anonymous nature of the internet usage has led to severe disadvantages. There has been an increasing cyber related crimes, Cyber law is imperative to a nations' internal & external security.

Types of cyber crime

1. using computer to attack other computers such as hacking , virus attack , DOS attacks etc
2. using computer as a weapon – such as pornography ,Cyber Terrorism , credit card violations , IPR violations , EFT frauds

Cyber law -Cyber law means the legal issues related to use of communications technology particularly cyber space

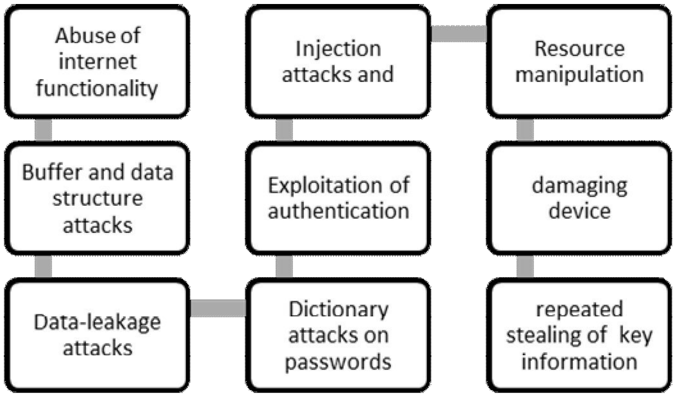
The IT Act 2000 - The IT Act 2000 attempts to change outdated laws and provides approaches to deal with cyber-crimes. The Act offers the legal framework so that information is not denied legal sanctions t, validity or enforceability, solely on the ground that it is in the form of electronic records. In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature. From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law. Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act. Digital signatures have been given legal validity and sanction in the Act. The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates. The Act now allows Government to issue notification on the web thus heralding e-governance. The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.

The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date. Under the IT Act, 2000, it shall now be possible for corporate to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

Hacking & related frauds: There are several types of frauds related to Hacking & related frauds. (Brain Krebs -Spam Nation: The Inside Story of Organized Cybercrime — from Global Epidemic to Your Front Door 2014).

Diagram-1 shows the types of cyber related anti-social activities. Abuse of functionality, Buffer and data structure attacks, Data-leakage attacks, Dictionary attacks on passwords, Exploitation of authentication, Injection attacks and, Resource manipulation etc are some of the cyber space misuse cases reported.

Diagram-1


Abuse of internet functionality
Buffer and data structure attacks
Data-leakage attacks
Injection attacks and
Exploitation of authentication
Dictionary attacks on passwords
Resource manipulation
damaging device
repeated stealing of key information

The expansion of internet technology is causing a lot of problems leading to cybercrime. The anonymous nature of the internet usage has led to severe disadvantages. There has been an increasing cyber related crimes, Cyber law is imperative to a nations' internal & external security. with the rise in terrorist activities Cyber laws has acquired importance worldwide. Cyber is very technical & it has legal perspectives.

Table-1 shows the relative magnitude of impact of cyber violation.

Sl	category	effects
1	attrition	damaging device
2	malware	interrupting normal computer functioning
3	hacking	data resource damaging
4	social texting	phishing
5	improper usage	installation of unauthorized software
6	equipment theft	stealing identity
7	wrong applications	harming computer working

The Nation Crime Records Bureau (NCRB): The Nation Crime Records Bureau (NCRB), Ministry of Home Affairs has released Cyber Crime Statistics for the 2013 year, which again shows rapid increase in cybercrime by 50% on year to year basis from 2012 to 2013. The statistics mainly show cases Registered under Cyber Crimes by Motives and Suspects (States & UTs): The maximum offenders came from the 18-30 age group. Among states, the highest incidents of cybercrime took place in Maharashtra (907) followed by Uttar Pradesh (682) and Andhra Pradesh (651). he maximum cybercrime arrests of four hundred twenty six (426) under the IT Act took place in Maharashtra and Andhra Pradesh was a distant second with 296 arrests, followed by Uttar Pradesh with 283 arrests. In percentage terms, the state that saw the most dramatic increase in cases registered under the IT Act was Uttarakhand at 475% (from 4 cases to 23); Assam a close second with 450% (from 28 cases to 154). Interestingly, the picture postcard union territory, Andaman and Nicobar islands, registered an eye-popping increase of 800% (two cases in 2012 to 18 in 2013) in the same category. The Delhi city has registered 131 cases of cybercrime cases which is an increase of 72.4 percent as compared to last year 2012. Whereas Lakshadweep, Dadar and Nagar Haveli reported no cybercrime cases for the year 2013. Also Cyber Crime activities seem to rare in the northeastern states. In 2013, only Age group classification - There were 3300 reported cases of cybercrimes in 2013 -2014.

l	details of fraud
1	tampering computer source documents
2	hacking with computer systems
3	obscene publication in electronic form
4	decrypting information
5	unauthorized access to
6	digital signature certificate frauds
7	breach of confidential security
8	breach of privacy
9	false electronic evidences
10	misrepresentation of documents through electronic media
11	creating loss to computer devices sources
12	counterfeiting
13	suppression of digital facts

Source : https://www.hsbc.gr/1/2/gr/en/.../ways.../internet.../security-guidelines

Considerations: There is a need to understand & identify the necessity of increasing cyber related crimes in India. The Governments both state & central should join hands in regulating cyber related crimes.

Table-3: cases of cybercrimes in 2013 -2014.

age group	average crimes
between 15-25	42%
between 25-35	35%
between 35-45	32%
between 45-55	18%
between 55-65	19%

Developing human resource - Developing human resource through education and training programs developing human resource -providing training for detection of cyber-crimes. cyber-crimes investigation training for youth at college level

Promotion of research and development - Promotion of research and development in cyber security.

Formulation of clear encryption laws - need for formulation of clear encryption laws

1. Strengthening CERT- computer emergency response team CERT has to be strengthened
2. International ATM heist - International ATM heist has to be set up on the lines of European countries
3. Quicker investigation of corporate scam -corporate scam has to be investigated quickly This ensures the Cyber criminals to disengage in criminal activities.
4. cloud computing - Legal & regularity in cloud computing has to be established
5. email policy has to be redefined
6. on-line payments has been received with frauds unforeseen in earlier years. There is a hike in online payment frauds. E commerce rules have to be redefined
7. online gambling has to be checked
8. illegal online pharmacies have to be checked
9. website blocking has to be checked
10. Money laundering , hawala transactions etc have to be checked
11. Mobile applications needs to be regulated
12. Cyber insurance policy- Companies in a bid to control cybercrime are shifting towards Cyber Insurance policies. Globally there is a great demand for Cyber insurance policies.

Strategy to secure cyber space: To design and implement a secure cyberspace, some stringent strategies have been put in place. This chapter explains the major strategies employed to ensure cyber security, which include the following:

1. Creating a Secure Cyber Ecosystem
2. Creating an Assurance Framework
3. Encouraging Open Standards
4. Enable systems incorporations,
5. Provide a medium for users to measure new products or services,

6. Organize the approach to arrange new technologies or business models,
7. Encouraging all organizations, whether public or private, to designate a person to serve as Chief Information Security Officer (CISO) who will be responsible for cybersecurity initiatives.

8. Indian Armed Forces are in the process of establishing a cyber-command as a part of strengthening the cyber security of defense network and installations.

9. Effective implementation of public-private partnership is in pipeline that will go a long way in creating solutions to the ever-changing threat landscape.

Conclusion- Technology has increased the methods and possibilities of commission of traditional and modern crimes. A person sitting in one part of the world may commit a cyber crime in another part of the world. has created unique law enforcement related problems as a given act or omission may be illegal in one country and may be legal in another.

References

1. Kulwant Rai Gupta – Liberalization & Globalization Of Indian Economy Atlantic Publishers 1995
1. Patrick Engerbretson The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy 2011
2. Kevin & William Simon -Ghost in the Wires: My Adventures as the World's Most Wanted Hacker 2011
3. Bruce. S. Secrets and Lies: Digital Security in a Networked World 2004
4. Brain Krebs -Spam Nation: The Inside Story of Organized Cybercrime — from Global Epidemic to Your Front Door 2014
2. https://en.wikipedia.org/wiki/Internet_Security_Awareness_
3. https://www.staysafeonline.org/ncsam/
4. https://www.hsbc.gr/1/2/gr/en/.../ways.../internet.../security-guidelines
5. www.dhs.gov › Get Involved
6. www.infosecawareness.in/
7. www.cyberlawsindia.net/internet-crime.html
8. infosecawareness.in/cyber-crime-cells-in-india