ORIGINAL RESEARCH PAPER

Commerce

CYBER CRIME, CYBER LAW AND CYBER SECURITY

KEY WORDS: Cyber crime, cyber law, cyber security, cyber terror, regulations, organization

Dr. Kalpesh B. Gelda

Adhyapak Sahayak (Assistant Professor) City C.U.Shah Commerce College

ABSTRACT

Today in the 21st Century the cyberspace has become an essential part of daily routine and vehicle for change. While rapid technological developments have provided vast areas of new opportunity and potential sources of efficiency for organizations of all sizes, these new technologies have also brought unprecedented threats with them. The Telecommunications, Commercial, Industrial, Financial systems, Service and Regulations are totally dependent on interconnect cyber system to operate and plan the system. The solution brings crime or negative impact with it as a very well known saying. Cyber Crime destroys or mainly attacks people or organizations or society financially or reputably, unlike in traditional crime here it damages physically. World is witnessing in the present arena and reports are also depicting and increasing trend of cyberspace and cybercrime. Organizations and people need to pace up themselves to implement appropriate and adequate security to negate these cyber crimes. In a report published by the National Crime Records Bureau report (NCRB 2011), the incidence of cyber crimes under the IT Act has increased by 85.4% in the year 2011 as compared to 2010 in India, whereas the increase in incidence of the crime under IPC is by 18.5% as compared to the year 2010. Visakhapatnam records the maximum number of incidence of cases. Maharashtra has emerged as the center of cyber crime with maximum number of incidence of registered cases under cyber crimes. Hacking with computer systems and obscene publication were the main cases under IT Act for cyber crimes. Maximum offenders arrested for cyber crimes were in the age group 18-30 years. 563 people in the age group 18-30 years were arrested in the year 2010 which had increased to 883 in the year 2011.

INTRODUCTION:

With the growing use of technology particularly in the corporate world is the need of an hour. These has resulted and given birth to different types of cyber crime lie virus, phishing, data theft etc. To countermeasures these crimes the government of various countries around the world has come up with various federal laws and regulations except Russia. Along with this various professional bodies have taken initiatives to set up formal forum to enhance the knowledge of the people in this era. Standards measures have also been drawn which can be used by organizations, people, society, etc. With the use and dependence on computer more and more in our daily life a new form of crime has emerged in the modern era which is known as cyber crime. Cybercrime include hacking, data theft, identity theft, cyber terrorism, internet fraud, terrorism funding, online fraud, data diddling, phishing/wishing, web defacement, denial of service, virus and worms, email spoofing, email bombing, pornography, software piracy, digital signature etc.

WHAT IS CYBER CRIME?

Cyber crimes can be defined as the unlawful acts where the computer is used either as a tool or a target or both. The term is a general term that covers crimes like phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, Spam and so on.

Cyber crime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It also covers the traditional crimes in which computers or networks are used to enable the illicit activity.

REASONS WHY THE PEOPLE/CORPORATE BECOME THEVICTIM OF CYBER CRIME:

- Installed the firewall and devices not monitored by the corporate security team
- Merging and Information Technology with the Information Security
- Non-allocation of enough budget in Information security
- Non-review and update of Information Security Policies
- Not defining the role and responsibilities of security organization
- No training to employees with respect to Security Technologies

SOURCES OF CYBER ATTACK:

INSIDERS	OUTSIDERS
• Current employees	• Terrorists Organized Crime
• Former employees	• Competitors
• Current service providers/consultants/contractors	• Information Broker
• Former service providers/consultants/contractors	• Activists/Hackers
• Business partners	• Foreign States/entities
• Customers	• Many others
• Suppliers	

TYPE OF CUBER CRIMES:

Sr. No.	TYPE	HOW CRIME IS DONE?	WHICH SECTION IS APPLIED?	PUNISHMENT
1	Unauthorized Access and Hacking	It is the practice of gaining the access to the computer system or their feature or data or information or modifying/deleting the same without the permission of their owner or person managing.	Section 43(a) of Information Technology (Amendment) Act 2008 read with Section 66	Penalty of Rs. 5 lakhs or imprisonment of 3 years or both
2	Data Theft	Data theft means stealing company data without their permission and this can be done through USB, E-mail etc.	Section 43(b) of Information Technology (Amendment) Act 2008 read with Section 66	Penalty of Rs. 5 lakhs or imprisonment of 3 years or both

3	Virus	These threats can be transmitted using E-mail services specially the e-mails containing the link or may also in the attachment.	Section 43(c) of Information Technology (Amendment) Act 2008 read with Section 66	Penalty of Rs. 5 lakhs or imprisonment of 3 years or both
4	Email Spoofing	It means or appears that the emails have been sent from one source but in actual it is sent from another sources.	Section 66D of Information Technology Act 2008	Penalty of Rs. 1 lakhs or imprisonment of 3 years or both
5	Email Spamming	It means the sending the same email to thousands of recipient.	There is no provision in the IT Act	There is no provision in the IT Act
6	Website Defacement	Website defacement is an attack on a website that changes the visual appearance of the site or a webpage.	Section 65 of Information Technology Act 2008	Penalty of Rs. 2 lakhs or imprisonment of 3 years or both
7	Email Bombing	Sending the same identical message multiple times to a particular address.	Section 66A of Information Technology Act 2008	Penalty of Rs. 5 lakhs or imprisonment of 3 years or both
8	Denial of Services	Flooding the network and causing disruption in connection between the server and node.	Section 43(f) of Information Technology (Amendment) Act 2008 read with Section 66	Penalty of Rs. 5 lakhs or imprisonment of 3 years or both
9	Pornography / Pedophiles	Printed or visual material containing the explicit description or display of sexual organs or activity, intended to stimulate sexual excitement.	Section 67 of IT Act	Penalty of Rs. 10 lakhs or imprisonment of 5 years or both for the first time. Penalty of Rs. 10 lakhs or imprisonment of 7 years or both for the second time.
10	Credit/Debit Card fraud	Use of stolen Credit/Debit Card or their information or use of fake Credit/Debit Card is common now-a-days to commit forgery or deducting small amount or any corporate fraud.	Section 43(a)(b)(g) of Information Technology Act 2008 read with Section 66	Penalty of Rs. 5 lakhs or imprisonment of 3 years or both
11	Data diddling	Data diddling involves changing data prior or during input into a computer. In other words, the data is not entered in the system in the way it should have been entered.	Section 43(d) of Information Technology (Amendment) Act 2008 read with Section 66	Penalty of Rs. 5 lakhs or imprisonment of 3 years or both
12	Illegal Online Selling	Compliance with law applicable to the business of organization is basic need. If the same violated or not complied using cyberspace then the organization ends up committing the crime which is in the nature of cyber. Like trading of wildlife, weapons, drugs, etc.	No Provision in IT Act but can be prosecuted under Arms Act	No Provision in IT Act but can be prosecuted under Arms Act
13	Defamation/ Smearing	Injuring of a person's good name or reputation using the cyberspace.	No Provision in IT Act but can be prosecuted under Indian Penal Code	No Provision in IT Act but can be prosecuted under Indian Penal Code
14	Cyber Stalking	Constantly sending the message to harass the recipient emotionally.	No Provision in IT Act but can be prosecuted under Indian Penal Code	No Provision in IT Act but can be prosecuted under Indian Penal Code
15	Cyber Terrorism	It is an activity of potentially attacking the large number of people in cheaper methods than traditional. It is the act of doing real world crime using cyberspace.	Section 66F of IT Act	Imprisonment up to life
16	Confidentiality, Integrity and Availability (CIA)	Violation of the rights of CIA that leads the cybercrime if done using cyberspace.	Section 43 of Information Technology Act 2008	Penalty of Rs. 5 lakhs or imprisonment of 3 years or both
17	Phishing/Vishing	Fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online.	Section 43 of Information Technology (Amendment) Act 2008 read with Section 66D	Penalty of Rs. 1 lakhs or imprisonment of 3 years or both

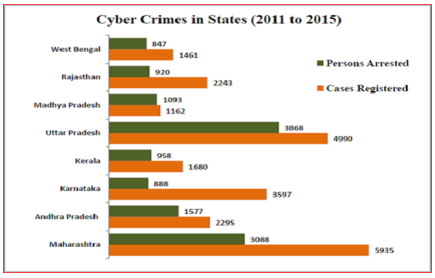
There are many other cybercrimes which can be committed and may not come under aforementioned classification but can be prosecuted under IT act or other relevant act.

GROWTH OF CYBER CRIME CASES IN INDIA:

ASSOCHAM – Mahindra SSG Report, Jan 2015 revealed that in the past attacks have been mostly initiated from the countries such as US, Turkey, China, Brazil, Pakistan, , Algeria, Europe and the UAE, and with the growing adoption of internet and smart phone India has emerged as one of the most favorite countries among cyber criminals.

Year	IT Act		IPC	
	Cases Registered	Persons Arrested	Cases Registered	Persons Arrested
2011	1791	1184	422	446
2012	2876	1522	601	549
2013	4356	2098	1337	1203
2014	7201	4246	2272	1224
2015	8045	5102	3422	2867
Total	24269	14152	8054	6289

The numbers of cases registered under the IT Act and IPC have been growing continuously. The cases registered under the IT act grew by more than 350% from 2011 to 2015. There was almost a 70% increase in the number of cyber crimes under the IT act between 2013 and 2014. The cases registered under the IPC increased by more than 7 times during the period between 2011 and 2015. Similar trend is observed in the number of persons arrested. The government also acknowledges the increase in the number of such crimes and that the introduction of technologies, devices including smart phones and complex applications, and rise in usage of cyber space for businesses has resulted in such an increase.



The list of states with the highest incidence of cyber crime for the period 2011 to 2015 throws no surprises. Maharashtra tops the list with more than 5900 cases in the 5 years followed by Uttar Pradesh with close to 5000 such cases. Karnataka is third with more than 3500 cases. The top states in this list are the ones with a greater internet subscriber base. The bottoms 10 are relatively smaller states with lower population & lower internet penetration.

CYBER SECURITY:

Before understanding and gaining the knowledge of the cyber security it is very much important to know why the cyber security is must in today's world and what consequences one can face if proper security is not incorporated in the system.

CONSEQUENCES OF CYBER SECURITY:

- Data/Information may get destroyed, stolen or exposed
- System availability may be denied or degraded
- Present or former employees or customers may get personally impacted
- Lawsuits
- Damage to Corporate Brand image

INITIATIVE BY GOVERNMNET:

- Cyber Crime Cell has been set up in all the Indian States and Union Territories for reporting and investigation of Cyber crime.
- Reserve Bank of India (RBI) has issued a circular to all Commercial Banks on phishing attacks and Credit Card operations.
- RBI has also to take preventive/detective measures to tackle phishing attacks. RBI has also advised bans to leverage technology to support business processes and implement all stipulations outlined by RBI from time to time. Bans have been advised to set up internal control system to combat frauds and to take proactive fraud control and enforcement measures.
- Formation of Institute or Cell or Association like

- Data Security Council of India (DSCI)
- NASSCOM
- Indian Computer Emergency Response Team (CERT)
- Centre for Development of Advanced Computing (CDAC)
- Information Sharing and Analysis Centers (ISACs)

SECURITY:

1) Do not leave the unencrypted data (words, images, reports etc.) in the email boxes.
2) Complying with requirements of laws (HIPAA, SOX, etc.) is not enough to secure your data, it is equally important to follow standards issued by various International bodies lie ISACA, ISO, ICAI, IIA etc.).
3) Security Assessment and build roadmap with the help of standards like ISO 27001.
4) Involvement of Top Level Management and enough budget and resources.
5) Review and update of security policies, procedures and supporting resources.
6) Design and regular testing of business continuity plans and disaster recovery plans.

CONCLUSION:

The above steps are only illustrative and not exhaustive; organization may deploy additional security measures according to their need to protect their valuable assets – Intellectual property, People Information, Financial Information and Business Information.

The success, Growth and Financial soundness of any organization can be said only by assessing the organization and how well their cyberspace is secured and protected.

REFERENCES:

1. www.data.gov.in
2. www.timesofindia.com
3. www.cyberlawclinic.org
4. www.newsindianexpress.com
5. www.rsublication.com
6. www.slideshare.net
7. http:wikipedia.org
8. www.cyberlawsindia.net