Cyber Crime, Cyber Law and Cyber Security

Today in the 21st Century the cyberspace has become an essential part of daily routine and vehicle for change. The Telecommunications, Commercial, Industrial, Financial Systems, Service and Regulators 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 organisations or society financially or reputably, unlike in traditional crime where it damages physically. World is witnessing in the present arena and reports are also depicting the increasing trend of cyberspace and cybercrime. Organisations and people need to pace up themselves to implement appropriate and adequate security to negate these cyber crimes. Read on...

Cyber Crime

There is no single definition of cyber crime but it can be generally termed as any unlawful or criminal activity done with the help of computer system, communication devices, Internet, Network, Cyberspace and web. There are crimes that are only committed on the Internet and are created exclusively because of the World Wide Web.

Now-a-days, Cloud computing has become more popular among the people and corporate which concentrates and encompasses more and more sensitive data. Inadequate security makes it vulnerable to cybercriminals.

CA. Mushir Ahmed Shaikh

(The author is a member of the Institute. He can be reached at mashaikh1991@gmail.com.)

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.

History of Cyber Crime

During the era of 1820, when Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom device which uses the repetition of a series of steps in the weaving of special fabrics. This act of advancement in the textile industry was new and the employees of the organisation got perplexes. They started to feel uneasy and felt that their employment is in risk and daily bread or livelihood might be threatened. This causes the panic among them and committed the act of sabotage to destroy the Joseph-Marie Jacquard use of technology in future.

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.

Then the case of Ian Murphy added more flavor on this topic, in which Murphy broke into the computer and manipulated with the computer billing date so that the customer can receive the products at discounted rates during the normal business hours.

Another case when cashier of one of the bank of New York used the computer to embezzle over two million dollars.

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 like 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 setup formal forum to enhance the knowledge of the people in this era. Standards measures have also been drawn which can be used by organisations, people, society, etc.

Initiative by Government:

- 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 Banks to leverage technology to support Business processes and implement all stipulations outlined by RBI from time to time. Banks 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-In), Centre for Development of Advanced Computing (CDAC), Information Sharing and Analysis Centers (ISACs)

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:

i) Data/Information may get destroyed, stolen or exposed
ii) System availability may be denied or degraded
iii) Present or former employees or customers may get personally impacted
iv) Lawsuits
v) Damage to Corporate/Brand Image

Security:

i) Don't leave the unencrypted data(words, images, reports, etc) in the email boxes
ii) Complying with requirement of laws (HIPAA, SOX, etc) is not enough to secure your data, it is equally important to follow standards issued by various International bodies like ISACA, ISO, ICAI, IIA, etc)
iii) Security Assessment and build roadmap with the help of standards like ISO 27001
iv) Involvement of Top level management (BOD) and enough budget and resources
v) Review and update of Security policies, procedures and supporting resources
vi) Design and regular testing of business continuity plans and disaster recovery plans

The above steps are only illustrative and not exhaustive; organisation 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 organisation can be said only by assessing the organisation and how well their cyberspace is secured and protected.

Source of Attack:

Insider: Current employees, former employees, Current service providers/consultants/contractors, former service providers/consultants/contractors, Suppliers, Business partners and customers

Outsider: Terrorists organised Crime, competitors, Information broker, activists/hackers, foreign states/ entities and many others.

Reason why the people/corporate become the victim of Cyber crime:

i) Installed the firewall and devices not monitored by the corporate security team
ii) Merging the Information Technology with the Information Security
iii) Non-Allocation of enough budget in Information security
iv) Non-review and update of Information security policies
v) Not defining the role and responsibilities of security organisation
vi) No training to the employees with respect security technologies

Category of Cyber Crimes:

1) **Unauthorised Access & 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.
Hacking tools: Ping of death, netstat live, hacker evolution, Advance port scanner, etc
The person who is accused of the above can be prosecuted under section 43 (a) of Information Technology (Amendment) Act 2008 read with section 66 which prescribe the penalty of fine which may extend to ₹5 lakhs or imprisonment which may be extend to three years or with both.
2) **Data Theft:**
Data Theft means stealing company data without their permission and this can be done through USB, E-mail, Etc. Data Theft also includes copying or stealing the web pages of the company Data Theft Protection tool: Falconstor Continuos data protector, McAfee Data Loss Prevention, PKware partner Link, RSA Data Loss Prevention Suite, Websense's Content Protection Suite, etc.
The person can be prosecuted under Section 43 (b) IT Act read with section 66. The penalty is of fine which may extend to ₹five lakhs or imprisonment which may be extend to three years or with both.
3) **Virus**
According IT (Amendment) Act, 2008 "Computer Virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource
These threats can be transmitted using e-mail services specially the e-mails containing the link or may also in the attachment. The best remedy is firewall, regular updating of anti-virus
These offence can be prosecuted under Section 43(c) and (e) read with section 66 of IT (A) Act, 2008 and Punishment of imprisonment which may extend to three years or fine which may extend to ₹Five lakhs or both
4) **Email Spoofing:**
It means or appears that the email have been sent from one source but in actual it is sent from another sources
Section 66D of IT act prescribes the punishment which may extends to three years of imprisonment and fine may extend to ₹one lakhs)
5) **Email Spamming:**
It means the sending the same email to thousands of recipient.
There is no provision in the IT act for email spamming. This is the loophole in the law that regulator have not considered this an serious issue or it is may be due to negligence. When after the death of Mr. Bal Thackeray two young women were arrested for posting alleged offensive messages on the social media under section 66A then why not email spam is an issue.
6) **Website Defacement:**
According to Wikipedia Website defacement is

an attack on a website that changes the visual appearance of the site or a webpage. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own.

Section 65 of IT Act prescribes the punishment upto three years of imprisonment or fine which may extend to ₹ two lakhs or both)

7) **Email Bombing:** Sending the same identical message multiple times to a particular address

Section 66A of IT Act, imprisonment may extend to three years or fine upto ₹ five lakhs or both)

8) **Denial of services:**

Flooding the network and causing disruption in connection between the server and node

Section 43(f) read with section 66 of IT act, imprisonment may extend to three years or fine upto ₹ five lakhs 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 says that for the first time conviction imprisonment may extend to five years and fine of ₹ ten lakhs and for second or subsequent conviction imprisonment may extend to seven years and fine may extend to ten lakhs)

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 deducing small amount or any corporate fraud.

Section 43 (a) (b) (g) read with section 66 of IT act, which prescribes the punishment of imprisonment which may extend to three years or fine upto ₹ five lakhs 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) read with section 66 of IT act, which prescribes the punishment of imprisonment which may extend to three years or fine upto ₹ five lakhs or both

12) **Illegal online selling**

Compliance with law applicable to the business of organisation is basic need. If the same violated or not complied using cyberspace then the organisation ends up committing the crime which is in nature of cyber. Like trading of wildlife, weapons, drugs,etc.

No provision in IT act but can be prosecuted under Arms Act, etc.

13) **Defamation/smearing:**

Injuring of a person's good name or reputation using the cyberspace

No specific 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

15) **Cyber Terrorism:** It is an activity of potentially attacking large number of people in cheaper methods than traditional. It is act of doing real world crime using cyberspace.

Section 66F of IT act prescribes that punishment of imprisonment which may extend for Life

16) **CIA (confidentiality, Integrity and Availability)**

Confidentiality means non-disclosure of Information to the unauthorised person.

Integrity means prevention unauthorised additions, deletions or alterations.

Availability means information should be accessible at the time of need.

Violation of above said rights leads the cybercrime if done using cyberspace.

Section 43 of IT act, prescribed that punishment of imprisonment which may extend to three years or fine upto ₹ five lakhs 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 read with section 66D of IT act, which prescribes the punishment of imprisonment which may extend to three years and fine of ₹ one lakhs

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. The core part of cyber crime is the usage of cyberspace whether it is done to commit real world crime or to attack other computers or system devices or network.

Information Technology

CASES CAN ALSO BE REGISTERED UNDER IPC and THOSE INCLUDE:

- Offences by/against Public Servant (Section 167, 172, 173, 175 IPC)
- False electronic evidence (Section 193 IPC)
- Destruction of electronic evidence (Section 204, 477 IPC)
- Forgery (Section 463, 465, 466, 468, 469, 471, 474, 476, 477A IPC)
- Criminal Breach of Trust (Section 405, 406, 408, 409 IPC)
- Counterfeiting Property Mark (Section 482, 183, 483, 484, 485 IPC)
- Tampering (Section 489 IPC)
- Counterfeiting Currency/Stamps (Section 489A to 489E IPC)

FEW CASE LAWS:

1) **Frios v/s State of Kerala**
   Facts: In this case it was declared that the FRIENDS application software as protected system. The author of the application challenged the notification and the constitutional validity of software under Section 70. The court upheld the validity of both.
   It included tampering with source code. Computer source code the electronic form, it can be printed on paper.
   Held: The court held that Tampering with Source code are punishable with three years jail and or two lakh rupees fine of rupees two lakh rupees for altering, concealing and destroying the source code.
2) **Syed Asifuddin case:**
   Facts: In this case the Tata Indicom employees were arrested for manipulation of the electronic 32- bit number (ESN) programmed into cell phones theft were exclusively franchised to Reliance Infocom.
   Held: Court held that Tampering with source code invokes Section 65 of the Information Technology Act.
3) **Case law:** Just Dial V/s Infomedia Delhi HC Dell Computer V/s Commissioner of Custom 2005 Tribunal Bangalore: It was held the Department was not allowing the exemption under notification issued in 2003 on the security protection taken by the Dell for Theft of data by both Internal and External Agencies. The Court the given the verdict in favor of Dell.
4) **Case Laws on hacking:** Sanjay Kumar v/s State of Haryana (10/01/2013) CRR No. 66 of 2013:
   Where the employee of the software vendor has manipulated the bank software source code and embezzled the mammoth amount of nearly ₹17 lacs.
   The bank was the customer of the software company.
5) **Arif Azim case**
   Summary of the case:
   Arif Azim case was India's first convicted cyber crime case under IPC. Case pertaining to the mis-use of credit card. Arif Azim used the credit card information of some other person and successfully made the transaction and made online shopping. The case came into the limelight when after the month of purchase real credit card holder denied the transaction.
6) **Juvenile accused:**
   A student of class eleven created the website with vulgar remarks about his classmate.
7) **Defamation**
   The case pertaining to posting of obscene, defamatory and annoying message about the divorcee woman in the yahoo message followed by annoying phone calls and e-mail.
8) **Threatening e-mail**
   Private new channel claimed that they received e-mail in which sender has threatened to blow up the andheri railway station. Eventually found out that sender was 16 year old student from Ahmadabad.

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, Turkey, Europe, and the UAE, and with the growing adoption of internet and smartphone India has emerged as one of the most favorite countries among cyber criminals.

Cases registered under IT Act of Cyber crime during 2013:

Top 10 States:

State/Uts	1 Maharashtra	2 Andhra Pradesh	3 Karnataka	4 Uttar Pradesh	5 Kerala	6 Madhya Pradesh	7 Rajasthan	8 West Bengal	9 Assam	10 Punjab
Tampering Computer Source Documents	11	30	8	3	19	1	6	21	0	3
Loss/Damage to computer resource/ utility	246	330	247	75	73	226	124	112	42	73
Hacking	29	16	182	71	56	14	23	27	0	12
Obscene Publication/ transmitssion in electronic form	122	234	48	159	177	41	81	37	111	54
Faliure of compliance/ Orders of Certifying Authority	4	0	0	1	3	0	0	3	0	0
Faliure to assist in decrypting the information intercepted by Govt. Agency	2	0	0	3	1	0	0	0	0	0
Un-authorised access/attempt to access of protected Computer System	0	0	1	17	0	0	1	0	0	0
Obtaining Licence or Digital Signature Certificate By Misrepresentation/ supression of fact	3	0	1	3	1	0	0	1	0	1
Publishing false digital Signature Certificate	0	2	0	2	0	0	0	0	0	0
Fraud Digital Signature Certificate	2	13	16	12	2	0	2	0	1	3
Breach of confidentiality/ privacy	5	10	10	26	17	0	2	9	0	0
Other	257	0	0	0	0	0	0	0	0	0
Total	681	635	513	372	349	282	239	210	154	146

Source: www.data.gov.in

People become attached to their burdens sometimes more than the burdens are attached to them. - George Bernard Shaw