

Cyber Security : Indian perspective

Bharti Trivedi – PhD (Comp. Sc.)
Director – Apex Technology
Adjunct Associate professor – M. S. University

Agenda

- Introduction
- Cybercrime: Definition and Origins of the Word
- Cybercrime and Information Security
- Who are Cybercriminals?
- Classifications of Cybercrimes
- Cybercrime: The Legal Perspectives
- Cybercrimes: An Indian Perspective
- Cybercrimes and Cyber security: The Legal Perspectives
- Cyber laws
- The Need for Computer Forensics

Interesting Findings of the Indian Online 2011 report

- According to the annual I-Cube Report published by IAMAI (Internet and Mobile Association Of India), India's internet population is expected to grow to 121 million users by December 2011 from 100 million in September this year.
- 28% growth in Internet users (From 51 Mln last year to 65 Mln this year)
- Internet reaches 29 million Indian households
- Over 4 in 5 are 'daily' users. Daily users' base grew faster, at 33%
- 9 out of 10 'home' and 'office' based online Indians log on to the net 'daily'
- Net surfing is among top 3 favorite 'indoor entertainment' for 3 out of 4 of them
- 9 out of 10 of them (86%) use social media sites!

User Activities on Internet

Online Activity	% Internet Users Undertaking	% Change From last Year
Emailing	95%	+1%
Search or buy non-travel products	76%	+32%
Web info search (text, images)	74%	+22%
Download music	69%	-3%
Job search	62%	+6%
Social networking	61%	+8%
Search or buy travel products	59%	+25%
Instant messaging/chatting	57%	+1%
PC to mobile SMS	54%	-2%
Pay bills online	51%	+22%

Most used Websites by Users

Vertical	Top Website	% Use (Among Vertical Users)
Generic Portals (all-purpose websites)	Yahoo, Google	84%, 84%
Emailing	Gmail	92%
Instant Messaging	Gtalk/Gmail	73%
Job Search	Naukri	78%
Online News	Google	61%
Online Travel Buy	IRCTC	81%
Online Games	Facebook	51%
Online Buying (Non-Travel)	Ebay	49%
Real Estate	99acre	64%
Business & Financial News	Google	55%
Online Share Trading (Trading)	Sharekhan	50%
PC to PC Net Telephony	Google/Gtalk	89%
PC to Telephone Net Telephony	Google/Gtalk	69%
PC to Mobile Messaging (sms)	Way2sms	79%
Net banking	ICICI Bank	49%

Growing Concern

- Computing Technology has turned against us
- Exponential growth in security incidents
- Complex and target oriented software
- Common computing technologies and systems
- Constant probing and mapping of network systems

Why learn about CYBER CRIME ?

Because



- Everybody is using COMPUTERS..
- From white collar criminals to terrorist organizations And from Teenagers to Adults
- Conventional crimes like Forgery, extortion, kidnapping etc.. are being committed with the help of computers
- New generation is growing up with computers
- **MOST IMPORTANT - Monetary transactions** are moving on to the INTERNET

WHAT IS COMPUTER CRIME?

- All crimes performed or resorted to by abuse of electronic media or otherwise, with the purpose of influencing the functioning of computer or computer system.
- COMPUTER CRIME is any crime where –
 1. Computer is a target.
 2. Computer is a tool of crime
 3. Computer is incidental to crime

Profile of Cyber Criminal

- Discontented employees.
- Teenagers.
- Political Activist.
- Professional Hackers.
- Business Rival.
- Ex-Boy Friend.
- Divorced Husband. etc

Recent news on cyber crimes

(2011 sep)

- Victims of cyber crime lost £71 billion in total over the last year, according to global figures released today.
- Over half of the UK population fell victim to cyber crime in that time, with 19 being hit every minute, a Norton survey found.
- Yet nearly all studies have pointed to a significant rise in cyber crime cost. An HP study last month showed the average cost of cyber crime on companies rose 56 per cent over the last year

Cyber crime statistics 2011

(March 2011- Infographic)

- 75 million scam emails are sent every day claiming 2000 victims.
- 73% of Americans have experienced some form of cyber crime (65% globally)
- 66% of world hackers are Americans
- 10.5% are from UK
- 7.5 % are Nigerian
- Brazil suffers more than any other country with 83% of population having suffered from internet crime.

Top 5 cyber crime complinats

- Non delivery (paying for the merchandise online, but not receiving it)
- Auction fraud
- Debit/ credit card fraud
- Confidence fraud (advance fee fraud – Nigerian letters)
- Computer fraud

FBI -February 2011 study

1. Non-delivery Payment/Merchandise 14.4%
2. FBI-Related Scams 13.2%
3. Identity Theft 9.8%
4. Computer Crimes 9.1%
5. Miscellaneous Fraud 8.6%
6. Advance Fee Fraud 7.6%
7. Spam 6.9%
8. Auction Fraud 5.9%
9. Credit Card Fraud 5.3%
10. Overpayment Fraud 5.3%

VICTIMS

- Innocent
- Criminals and greedy people
- Unskilled & Inexperienced
- Unlucky people

Computer Crimes are Vulnerable

Because of :-

- Anonymity,
- Computer's storage capacity,
- Weakness in Operating System,
- Lack of Awareness of user

- A report in September from Symantec pointed out that while 58 per cent of infections were in Iran, about 18 per cent was in Indonesia and nearly 10 per cent in India.
- India is the eleventh most affected country by cyber crimes and with an aim to address some of the issues related to hacking and cyber warfare

Types of Cyber Crime

- HACKING
- DENIAL OF SERVICE
- VIRUS
DISSEMINATION
- SOFTWARE PIRACY
- PORNOGRAPHY
- IRC Crime
- Cyber squatting
- CREDIT CARD FRAUD
- Bot networks
- NET EXTORTION
- PHISHING
- SPOOFING
- CYBER STALKING
- CYBER
DEFAMATION
- THREATENING
- SALAMI ATTACK
- CROSS SITE
SCRIPTING (XSS)
- VISHING

Phishing email

From: *****Bank [mailto:support@*****Bank.com]

Sent: 08 June 2004 03:25

To: India

Subject: Official information from ***** Bank

Dear valued ***** Bank Customer!

For security purposes your account has been randomly chosen for verification. To verify your account information we are asking you to provide us with all the data we are requesting. Otherwise we will not be able to verify your identity and access to your account will be denied. Please click on the link below to get to the bank secure page and verify your account details. Thank you.

https://infinity.*****bank.co.in/Verify.jsp

***** Bank Limited

- **My father left me \$40 million in his will, but I have to bribe government officials to get it out**
- **The Nigerian National Petroleum Company has discovered oil, and we as officials of that company want to insider acquire the land, but we need an Indian front man to purchase it first for us**
- **We just sold a bunch of crude oil in Nigeria, but we have to bribe the banker to get it out**
- **The Nigerian government overpaid on some contract, and they need a front man to get it out of the country before the government discovers its error**
- **Nigerian 4-1-9 Scam**

Steps to check Cyber crime

- Even when one follows the latest security trends and goes for the best practices to protect the systems and networks, there are still many loopholes left in the network itself that gives into the cyber criminals. While IDC (International data Corporation), IPS (Intrusion detection system), Firewalls and Log Analysis are some of the state of the art cyber defenses available, network forensics is an evolving field in the security landscape.

Steps to check Cyber crime

- Data is recorded, stored and reconstructed in order to discover the source of security attacks or other problem incidents." This leads us to the unknowns in the security breach and hence to the truth. "And the truth is on the wire," said Pillai. To reach to the truth, the various tools used are archiving the network traffic, sessionizing, and parsing and data extraction.

computer forensics

- ... is the art and science of applying computer science to aid the legal process.
- *We define computer forensics as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.*

Indian Crime Scene

- The country has the highest ratio in the world (76 per cent) of outgoing spam or junk mail, to legitimate e-mail traffic.
- Over 86 per cent of all attacks, mostly via 'bots' were aimed at lay surfers with Mumbai and Delhi emerging as the top two cities for such vulnerability.
- India has now joined the dubious list of the world's top 15 countries hosting "phishing" sites which aims at stealing confidential information such as passwords and credit card details.
- A 23 year-old person from Tiruchi was arrested by the City Cyber Crime police on Thursday on charges of sending an e-mail threat to the Chief Minister and his family in 2007.

Indian Trends of Incidents

- Computer hackers have also got into the Bhabha Atomic Research Centre (BARC) computer and pulled out important data.
- Some computer professionals who prepared the software for MBBS examination altered the data and gave an upward revision to some students in return for a hefty payment.

Security of Information Assets

- Security of information & information assets is becoming a major area of concern
- With every new application, newer vulnerabilities crop up, posing immense challenges to those who are mandated to protect the IT assets
- Coupled with this host of legal requirements and international business compliance requirements on data protection and privacy place a huge demand on IT/ITES/BPO (IT/IT Enabled Services/ Business Process outsourcing) service organizations
- **We need to generate ‘Trust & Confidence’**

Cyber Security Strategy – India

- **Security Policy, Compliance and Assurance – Legal Framework**
 - IT Act, 2009
 - IT (Amendment) Bill, 2006 – Data Protection & Computer crimes
 - Best Practice ISO 27001
 - Security Assurance Framework- IT/ITES/BPO Companies
- **Security Incident – Early Warning & Response**
 - CERT-In National Cyber Alert System – Computer Emergency Response Team (Govt of India)
 - Information Exchange with international CERTs
- **Capacity building**
 - Skill & Competence development
 - Training of law enforcement agencies and judicial officials in the collection and analysis of digital evidence
 - Training in the area of implementing information security in collaboration with Specialised Organisations in US
- **Setting up Digital Forensics Centres**
 - Domain Specific training – Cyber Forensics
- **Research and Development**
 - Network Monitoring
 - Biometric Authentication
 - Network Security
- **International Collaboration**

Status of security and quality compliance in India

- Quality and Security
 - Large number of companies in India have aligned their internal process and practices to international standards such as
 - ISO 9000 – Quality management
 - CMM – Capital Maturity Model
 - Six Sigma
 - Total Quality Management
 - Some Indian companies have won special recognition for excellence in quality out of 18 Deming Prize winners for Total Quality Management in the last five years, six are Indian companies.

ISO 27001/BS7799 Information Security Management

- Government has mandated implementation of ISO27001 ISMS (Information Security Management system) by all critical sectors
- ISMS 27001 has mainly three components
 - Technology
 - Process
 - Incident reporting and monitoring
- 296 certificates issued in India out of 7735 certificates issued worldwide
- Majority of certificates issued in India belong to IT/ITES/BPO sector

Postal Address:

Indian Computer Emergency Response Team (CERT-In)
Department of Information Technology
Ministry of Communications & Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003

India If the purpose of your communication is vulnerability report, security alerts, or any other technical questions/feedback related to cyber security, contact CERT-In Information Desk.

Email: info@cert-in.org.in

Thank you