

CYBER CRIME-A NEW CHALLENGE FOR THE POLICE

- Balwinder Singh, Addl. Sec, Central Vigilance Commission, GOI,

INTRODUCTION

Computer Crime is just emerging as a major problem area for the law enforcement agencies in India. The current low incidence of computer crime in India is because computerisation of banks and other financial institutions and their networking is still on. The other sensitive sectors which would be vulnerable to cyber-crime are also still in the early stages of networking. But the scenario in the near future is likely to change significantly and rapidly.

AREAS OF CONCERN

The entire banking and other financial sector is in the process of massive computerization. The various crucial departments of both the Government of India and a large number of States are also moving in the same direction. The growth of Internet is mind boggling. In one year between 1998 and 2003, Internet users have increased from 22 lakh to 1500 lakh. This has a direct impact on growth of E-Commerce. Even today, one can purchase music cassette, books, cinema tickets, even vegetables and fruits on internet in Delhi and other metros of India. In India. Confederation of Indian Industries had projected a figure of B2B

(Business to Business) B 2 C (Business to Consumer) E-Commerce to the tune of Rs. 36,800 crore and Rs.25,000 crore respectively in the year 2003, i.e. just within one year. While the exponential growth of Internet would give great fillip to the Indian economy, its potential for credit card and other frauds cannot be underestimated. Cyber-terrorism is also emerging as a major threat to the nation. The critical infrastructure like telecommunications, airlines, railways, power sector are highly vulnerable to this threat.

NATURE OF COMPUTER CRIME

Computer Crime mainly consist of unauthorized access to computer systems, data alteration, data destruction, theft of intellectual property. Almost all computer crimes involve unauthorized access, or access exceeding the authorization. The hacker by stealing or bypassing the password and other security features breaks into the computer system. The intention may be to commit a financial fraud or to steal some sensitive data. At times, in cases of cyber-terrorism, the intention is to damage the computer system for disrupting telecommunication, railways,

power supply and other critical infrastructure.

SOME EXAMPLES OF CYBER-CRIME IN INDIA AND ABROAD

During the article, an overview of the techniques of committing computer crime like hacking, phreaking, logic bomb, Trojan horse, salami would be given. It would include a few cases of computer crime which have occurred abroad. The following case illustrates the vulnerability of on-line commerce. In California (USA) wherein a person named Salgado hacked into the computer of an Internet Service provider and committed theft of sixty thousand Credit Card numbers. The hacker was arrested and the case ended in conviction on the basis of evidence gathered by undercover techniques. Another case would illustrate threat to Internet banking system. In 1998, a major Bank fraud involving theft of US\$ 10 million was committed by a Russian named Vladymir Levin. While sitting in Russia, he hacked into computer system of a City Bank Branch in USA through an Internet connection and succeeded in breaking the security features of the Bank. Through Internet banking, he could move the cash from US to Argentina, Indonesia and Switzerland. Routine computerized audit system gave a lead and hacking was detected. The hacker was arrested when he visited Switzerland to collect cash from the Bank. Even in the Sept 9/11 bombings

in USA, Al Qaeda Terrorists transferred funds across the globe through e-banking. This case illustrates threats to Internet banking system.

As regards computer crime in India, a few examples would give an idea about the nature of cases which have occurred so far. In New Delhi Municipal Corporation, a private agency entrusted with the responsibility of preparing and collecting electricity bills, embezzled Rs. 6.5 crore by creating duplicate set of bills showing lower receipts. In railways Computerised Reservation System, a few cases of false accounting by wrongly categorizing upper class monthly tickets as second class seasonal tickets have come to notice. Telecom frauds are closely linked with computer frauds. As computers and communication have become intertwined, telecom systems become vulnerable to fraud by use of computers. In India, we have come across some cases of reversal of telephone meters by software manipulations to reduce billing and also diversion of lines to prevent billing.

The growth of Internet has also facilitated some of the traditional crimes like pornography, gambling, forgery etc. though, no instance of utilization of computers as tools for espionage has come to notice in India but given the low level of awareness of security features, this is an area of concern. In India, as networking has not yet taken place in a big way, most of the computer frauds

which have so far come to notice pertain to stand alone systems or at best Local Area Networks. The potential for computer crime increases in geometrical progression when remote accessing in big networks becomes feasible.

STRATEGY FOR TACKLING CYBER-CRIME

A comprehensive strategy to tackle the emerging problem of cyber-crime should have following components:-

- (i) Emphasis on adequate in-built security features in the computer system.
- (ii) Establishing legal framework and evolving investigative techniques to gather evidence.
- (iii) International cooperation.

Significant advances have been made in computer security both in hardware and software. Policy-makers, Information Technology Managers have to ensure that proper threat perception is made an adequate level of security features introduced in the computer networks of sensitive departments. There is urgent need to sensitise the computer users the security of the State about the security features and right practices. A leading consultancy firm M/s. Gartner Group in a recently published research paper has mentioned that though, presently, computer crime is largely limited to

embezzlement and extortion but already trends are evident that organized crime and terrorist groups would indulge in cyber-terrorism because it is inexpensive and relatively more difficult to trace and prove in a Court of Law.

As regards legal framework, most of the advanced countries have already framed adequate laws for functioning in the computerized environment. In the US, following laws have been enacted:-

- Computer Misuse Act, 1991
- Telecommunications Act, 1996
- Electronic Fund Transfer Act (EFT), 1996
- Data Collection Improvement Act, 1996
- Digital Signature Legislation, 1996
- Intellectual Property Protection Act, 1996
- Federal Trade Marks Dilation Act, 1996
- Electronic Communication Privacy Act [dealing with Electronic Mail (E-mail)]

In India, the Information Technology Act 2000 is in place. The main objective of the legislation is to facilitate electronic trade and commerce by providing legal authenticity to electronic records and establishing a regulatory framework. The act provides for penalties for computer

crimes. The also includes amendments in various other enactments like Indian Evidence Act, India Penal Code, Bankers' Book of Evidence, etc.

There is a general perception that because of lack of visual evidence (LOVE), the computer crime is difficult to detect and even more difficult to prove. While it is true to some, but growth of technology is making it more and more feasible to detect this crime. Computer professionals working in the area of computer security have developed highly sophisticated Intrusion Detection Tools and inbuilt auditing systems. Computer criminals leave behind a large electronic trail. Every time a computer criminal thinks that he has deleted a file from the computer what he has actually done is that he has removed a link between the data area of the file and the file name. In Bank Scam Cases in India, many files which were supposed to have been deleted by the accused were actually retrieved from the computer hard discs during the investigation. More and more in-built computer audit systems would ensure that evidence collection through technological means becomes possible.

Our efforts as law enforcement officials have to be on training the Investigators in proper procedures of seizure of evidence in computerized environment, its proper storage etc. the criminal justice

system would also have to ensure that the Prosecutors and the Judges are trained to understand and appreciate this evidence. Legal framework is already being provided to make such evidence admissible. Adequate number of specialized forensic examiners called CART examiners need to be trained who understand the techniques of data recovery from systems which are non-operational or even affected by virus or which are protected by data encryption. They should develop expertise in recovering erased data from discs and locate hidden files or disguised data.

INTERNATIONAL COOPERATION

Computer Crime especially Internet Crime by its very nature is a crime in a boundary-less world. As explained in the case of City Bank Fraud, it is quite possible for a person sitting in one country may defraud a Bank/Institution in another country and proceeds of crime move to third country. While technical solution for electronic tracing of the computer criminals are becoming more and more available, there is need to evolve mechanisms for legal cooperation by reaching at international agreements on common definitions of computer crimes, issues concerning jurisdiction and procedural laws, and extradition etc. We will have to strengthen bilateral, multilateral and global mechanisms for this purpose.

ISSUES FOR DISCUSSION

The policy-makers need to concentrate on the following issues:-

- Information Security strategies and protection of National Information Infrastructure.
- Organizational Structure of Computer Crime Investigation Teams.
- Training of Investigators & Prosecutors.
- Forensic Experts specializing in this area.
- Evolution of Legal Tools (undercover agents, etc.)
- Cooperation between Police Investigating Agencies and Industry (Computer/Telecom/Banking, etc.)



'Alert Interpol Constable.
It's another suspected death
from the Cursor virus.'

“Holding on to anger, resentment
and hurt only gives you tense
muscles, a headache and a sore
jaw from clenching your teeth.

Forgiveness gives you back the
laughter and the lightness
in your life”.

- Joan Lunden,
in Healthy Living Magazine