10

Cyber Crimes

If cyberspace is a type of community, a giant neighbourhood made up of networked computer users around the world, then it seems natural that many elements of a traditional society can be found taking shape as bits and bytes. With electronic commerce we witness electronic merchants, plugged-in educators and doctors treating patients online. It should not come as a surprise that there are cyber criminals.

As an unregulated medley of corporations, individuals, governments and educational institutions that have agreed to use a standard set of communication protocols, the internet is wide open to exploitation. There are no 'regulators' and this lack of law enforcement leaves net users to regulate each other according to the reigning norms of the moment. Community standards in cyberspace are vastly different from the standards found at the corner of a main street. Cyberspace is a virtual tourist spot where faceless, nameless con artists can work the crowds. The critical issues now facing us can be divided into two broad categories:

- Denial of Service Attacks: The criminal's goal is to cause damage to the system (hacking, cracking and sending malicious code viruses) or computer network.
- The computer is the target of attacks.

At this stage it is important to bring out a major difference in treatment in the first edition of the book and this edition. In the first edition, our endeavour was to show how the Information Technology Act, 2000, had made provisions for various illegal acts and we also described some of

these. We would now go into more specific questions regarding the ways the guilty can be punished and how the aggrieved parties can get redress. Questions of admissibility of evidence and the precautions that bankers should take would be referred to.

At this stage we need to point out that there is a great need for a very vigilant approach in the current phase. In a crisis situation very often guards are lowered and sometimes even routine checks are ignored. A very rigid attitude towards checks needs to be adopted and extra care needs to be taken to ensure that advantage is not taken of by certain rogue elements. Further, we must show that managements of financial institutions (FIS) are vigilant and that excesses of any sort are avoided. Board of Directors and more particularly the Independent Directors must closely watch these aspects and must show zero tolerance towards deviations. Board overview of risk management function is critical and crucial in the current situation.

A criminal act takes place when a particular enactment lays down penalties and offences. In addition to the IT Act, 2000, the Code of Criminal Procedure, The Indian Penal Code, the Evidence Act and the Bankers' Book of Evidence Act have a bearing on cyber crimes.

More than 50 per cent of 100 million computers are networked. One can imagine the magnitude of the challenge of preventing infiltration into computer systems and challenges to computer security and intellectual property.

Computer criminals comprise co-workers, insiders, disgruntled employees or even the lazy ones, competitors, crackers and hackers. Their attacks range from unauthorized access by employees to break-ins by intruders. Before proceeding further, it might be useful to give a brief note on 'Computer speak'.

Term Definitions:

- Hackers: Use illegal methods of accessing a computer.
- Crackers: Programmes to extract information and benefit from it.
- Stealers: Beg, borrow or steal—passwords and other critical information.

Computer crimes take several forms including sabotage, revenge, vandalisms, theft, eavesdropping and 'data diddling', credit card frauds, counterfeiting, bank embezzlement and theft of secret documents. Introducing 'worms'/viruses are other forms of computer crimes. The other serious possibilities are information attacks on military, central banks, electricity companies and softwares in use.

Why and how do they occur? The perceived anonymity and the huge financial gain could be the main reasons. Other reasons are as follows:

- Research and development expenses, for a competitor who steals the information, would be nil and would allow the competitor to go ahead in technology.
- Network administrators' laxity.
- Failure to monitor security programmes allows 'hackers' to access the networked system and crimes often go undetected.
- Disgruntled employees or those whose services are terminated could create a security breach.
- Social engineering is used to build a friendship with employees and gain access to information.
- Cryptographic keys can be figured out by timing the computers.
- Firewalls and system probing.
- 'Cracker' programme to identify passwords is used to try every word in the dictionary as a password.
- Network file used to share files between systems is exploited through well-known vulnerabilities.
- 'Sniffing' allows all traffic on a network to the sniffed to collect authorized password.
- Another method of virus infection is transmitted via word files. Word documents are embedded with viruses sent via email. There is no way to see that a document is infected until it is opened.

For the simplicity of analysis one could broadly group these points with reference to certain sections of the IT Act.

- Section 43 (a) lays down that a person who accesses or secures access to such computer system or network would be liable to pay damages by way of compensation not exceeding one crore of rupees to the person so affected.
- Section 43 (b) makes a person liable to pay damages for downloading copies or extract any data or information from such a computer.
- Introduction or causing any computer contaminant or computer virus into any computer system or computer network would be liable for paying damages.
- Causing damage to a computer deliberately.
- Any person who does any or all of the following is liable to be charged for committing a crime:

- Assisting another person to gain unauthorized access.
- Damaging a computer system.
- Manipulating the data for financial benefit.
- Transferring service charges to an account of a person who has not availed the service.

The idea is not to present an exhaustive summary of the provisions of the Act, but to make readers aware of the crimes that can be perpetrated and the penalties that are levied for such criminal acts. A word of caution is absolutely necessary. The broad categories listed previously are further broken down and various details emerge. Inserting a CD or a floppy may not be a criminal activity, but browsing could certainly be one. There are a number of interpretations and elaborations not only of these sections, but also of similar sections in other countries like UK or USA.

At this stage the impact of some of these criminal activities on the working of FIs needs to be examined. The BIS (Bank for International Settlement) in its report on 'Risks management for electronic banking' presents a list of various risks associated with banking activities. Table 10.1 presents a list of these criminal activities.

Table 10.1 Cyber Crimes and Their Effect

Criminal Act	*Possible Manifestation*	*Potential Effect*
Unauthorized system access	Hackers enters internal systems; confidential information is intercepted, data gets corrupted; systems crash.	Loss of data, theft of information, costs of repairing perceived insecurity of bank systems.
Employee frauds	Alteration of data in order to draw funds from general bank accounts; theft of smart cards.	Reimbursement customer losses; reconstruction of accurate data; legal or regulatory sanctions.
Counterfeiting of electronic money	Criminals alter or duplicate electronic money to obtain goods or funds.	Liability for falsified money. Replacing costs associated with a compromised system.
Repudiation of a transaction	Transaction completed but customer denies that transaction took place.	Possible loss of funds or legal expenses to prove that transaction was authorized.
Significant breach of security	Introduction of virus; illegal entry by a hacker.	Customers may discontinue the use of that product or service; affected customers may leave and others follow.
Money laundering	Misuse by criminals to engage in money laundering.	Legal sanctions for non-compliance.

Source: Summary of BIS Report on E-finance Risks.

Problems of Enforcement

The first question that comes up relates to admissibility of evidence. With respect to admissibility, the question is whether electronic records are admissible in a court of law. The distinction between 'Real' and 'Hearsay' comes into play. Real evidence is information generated by the computer itself with the use of software. Interest calculations done automatically fall into this category. Hearsay evidence is records produced by the computer that are copies of information fed into the computer by humans initially. It is presumed that 'in the absence of evidence to the contrary the courts will presume that mechanical instruments were in order at the material time'. Section 65B of the Evidence Act 1872 has similar provisions introduced by the IT Act 2000. The other relevant authority in this respect is Uncitral Model Law, which states that electronic documents cannot be rendered inadmissible merely because it is electronic in nature. And the unreliability has to be independently proven. Further, even if certain documents are not real, they do become admissible, as documents are prepared in the ordinary course of business. The rationale for this presumption is that these entries are used for other purposes too and that is a sufficient guarantee of the truth of the records' content.

One would like to briefly touch on the certified copy aspects in the Bankers' Book of Evidence Act. If for some reason the evidence is not considered real then the question of a certificate may arise. We are of the view that if the programme is the one used in the course of business and if the software were functioning properly, then it may be sufficient to meet the requirements of admissibility.

The other difficulty comes because of the investigation techniques used. A physical act (say, a dacoit grabbing cash from a teller at gunpoint) would lead to an investigation as in any criminal act. The police would visit the scene of the crime, collect information from eye witnesses and try to gather finger prints or any trails left by the dacoit. In the case of a similar crime committed with the help of a computer the trail would be so far fetched that it might be necessary to get the cooperation of half a dozen systems managers and computer users. It could be an extremely difficult process. There are, of course, peculiar questions relating to privacy and the missing substitute for a biometric eyewitness testimony or physical evidence or the existing evidence pointing to a particular person. The only clinching evidence would be the recovery of the computer.

Perhaps, the time has come to harmonize the procedures in investigation and give a much greater leeway to the authorities in carrying out the investigations.

The Bankers' Book of Evidence Act, 1891, was amended in 2002 for acceptance of digital evidence. However, to get it accepted as evidence the following requirements have to be complied with. A printout of entry or a copy of a printout shall be accompanied by the following:

- A certificate to the effect that it is a printout of such entry.
- A certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of:
    - The safeguards adopted by the system to ensure that data is entered or an authorized person performs any other operation.
    - Safeguards adopted to prevent and detect unauthorized change of date.
    - Safeguards available to retrieve data that is lost due to systemic failure or any other reason.
    - The manner in which data is transferred from the system to removable media like floppies, discs or tapes or other electromagnetic data storage devices.
    - Mode of verification in order to ensure that data has been accurately transferred to such removable media.
    - Mode of identification of data storage devices.
    - Arrangement and custody of such storage devices.

It would be extremely difficult to get such certificates and to bring the officers for cross-examinations.

To illustrate our point, e-details of a case in the UK has been discussed here. An American bank obtains unauthorized access to the confidential information contained in the website of a bank in the UK. The UK bank confirmed the details and telephoned the CEO of the US bank. The CEO laughed and is reported to have replied: 'We are doing you guys a favour by giving people access to your website.' When the bank asked its lawyers to review the case, some startling conclusions emerged: *(a)* since the UK bank was not complying with UK financial services and personal data protection laws, it might be the subject of compliance orders and fines; *(b)* alerting the national authority against an overseas hacker was not of much use; *(c)* the burden of proof in a criminal case in the US requires that a jury be persuaded beyond reasonable doubt that the defendant has committed an offence and securing the proof for such an act would be a formidable task; *(d)* the bank had to assess and gather evidence as to who owned the Intellectual Property Rights (IPRs) in the website. This would include the authors of its initial design because they would own it unless

the agreement with the bank stated that the bank was to be the owner. If they were acting as employees of the bank, the bank would own it. If however, they were acting as independent contractors, then each author would own whatever he or she had created.

A number of similar cases in the US can be referred to, where cyber crime and the subsequent treatment of these 'criminals' is not taken very seriously.

The waters get so muddy that institutions cannot be blamed for leaving the matters untouched. The solution would be for laws to be tailored to suit the requirements that are now emerging. It remains to be seen whether the laws will ever catch up with the rapid changes in technology. Commercial law is slow to catch up with the business malpractices.