Speech

Computer Crime - an Overview *

S. P. Talwar

It gives me great pleasure to be amidst the representatives of the financial sector, National as well as International law enforcement agencies who have gathered here at the National Seminar on Computer Related Crime to interact on the threats posed by risks in computerised environment.

The economic loss caused internationally by this type of crime is estimated to run into large sums. Although this is not the scenario in India at present, this is potentially a high risk area which we have to address with care and in a timely manner. The vulnerability of computer systems which support critical applications, whether in the area of defence or finance, makes it imperative that we acquaint ourselves with the means to prevent and combat this menace. Since banks would be one of the major targets of computer crime, it is necessary for us to have an idea of not only of the level of computerisation in the banking industry in India but also of the mechanisms that have been set in place to address the problems that would endanger the systems.

Before we take up the various issues relating to computer related crime, let me give a brief overview on computer crime.

What is Computer Crime?

One of the characteristic features of computer crime is its transnational character. Computer crimes often extend across national borders thanks to the technological growth in the industry that has made geographical borders insignificant. Remote access facilities have necessitated the harmonization of domestic laws and regulations in tandem with global prosecution needs. However, the precise definition of computer crime itself may vary from country to country.

Broadly, computer crimes are those that are committed either on a computer system or with the aid of such a system. A distinction is sometimes made between 'computer fraud', where the fraud involves the manipulation of computers, and 'computer crime' where a computer is used to commit a fraud. Since this seminar is concerned with 'Computer Related Crime', both types of crimes would be the focus of attention of the participants of this seminar.

Types of Computer Crimes

However, it is important not to lose sight of types of crimes that are often committed. The United Nations Manual on the Prevention and Control of Computer Related Crime[1] classifies such crimes into five categories.

The first and most important type of this is the committing of a fraud by manipulation of the input, output, or throughput of a computer based system. This is of special interest to the RBI which has been entrusted with the task of supervision of banks and financial institutions.

Input manipulation is the most common type and results in the changing of input data

such as deposit amounts in ledgers, limits in accounts, or face values of cheques. Output manipulation is achieved by affecting the output of the system such as the one entailing the use of stolen or falsified cards in ATM machines.

The most well-known throughput manipulation technique involves the process of rounding off of the sums being credited to different accounts and siphoning of the rounded off digits to another account. No system is fool-proof and fraudulent transfers have been reported in even highly automated and secure fund transfer systems such as the CHIPS of USA and CHAPS of UK.[2]

Among the other types of computer crimes, the major ones are :

- computer forgery, which involves changing images or data stored in computers,
- deliberate damage caused to computer data or programmes through virus programmes or logic bombs,
- unauthorized access to computers by 'hacking' into systems or stealing passwords, and,
- unauthorized reproduction of computer programmes or software piracy.

Characteristics of Computer Crime

The characteristics of computer crime are different from that of conventional crime, in that it is relatively easy to commit, difficult to detect and even harder to prove. It is a 'low risk, high reward' venture for the criminal, who, with basic skills and persistence, can easily move large sums of money across countries or enter and destroy valuable data and cause very high damage to the affected organisations.

Computer crime can often turn out to be a 'dark' crime because of the lack of information that law enforcers have on its incidence and spread. This is partly due to the fact that detection of such crime is often difficult and requires a high level of skills, and partly due to the fact that organisations often do not report these crimes for fear of adverse publicity on their systems and controls. One estimate made in 1992 suggested that only 5 per cent of the losses caused by computer crimes were actually reported.[3] This is a matter of great concern for all of us because this would imply that the magnitude of the problem could well turn out to be far greater than what is widely known to be the factual position and, therefore, requires greater resources for both detection and prevention than the existing available levels. At the same time, it is necessary not to create a scare about its extent in the absence of hard and verifiable evidence.

Status of Computerisation of Banks in India

Let me now present the current status of computerisation of banks in India.

The first initiative in the area of bank computerisation stemmed out of the landmark report of the two committees headed by the former Governor of the Reserve Bank of India and currently Governor of Andhra Pradesh, His Excellency, Dr. C. Rangarajan. One of these Committees, viz. the **Committee on the Mechanization of the Banking Industry (1984)** was set up for the first time to suggest a model for mechanisation of bank branches, regional /

controlling offices and Head Office. This had been necessitated by the explosive growth in the geographical spread of banking following nationalization of banks in 1969.

In the seventies', there was a fourfold increase in the number of branches, five-fold increase in advances and a six-fold increase in deposits. Mechanisation was seen as the best solution to the "problems inherent in the manual system of operations, their adverse impact on customer services and the grave dangers to banks in the context of increasing incidence of frauds." Based on a study of transaction volumes and purposes, the Committee made detailed recommendations on the model of mechanisation.

In the first phase of computerisation spanning the five years ending 1989, banks in India had installed 4776 ALPMs at the branch level, 233 minicomputers at the Regional/ Controlling office levels and trained over 2000 programmers/systems personnel and over 12000 Data Entry Terminal Operators. The Reserve Bank too had embarked upon an ambitious programme to bring about state-of-the-art technology in the clearing process and had introduced MICR clearing at 4 centres and computerized clearing settlement at 9 centres.[4]

Against this backdrop, the **Committee on Computerisation in Banks** was set up once again under Dr. Rangarajan's Chairmanship to draw up a perspective plan for computerisation in banks. In its report submitted in 1989, the Committee acknowledged the gains of the initial efforts and sought to move away from the stand-alone dedicated systems to an on-line transaction processing environment in branch banking. It recommended that the thrust of bank computerisation for the following 5 years should be to fully computerise the operations at both the front and back offices of large branches then numbering around 2500.

Computerisation efforts among the Public Sector Banks (PSBs) in India, which account for over 80 per cent of the assets of the entire banking system, has been substantial. Of the 45,439 branches of the PSBs as on September 30, 1998, as many as 3,668 branches serving customers directly had been fully computerised with a complement of more than 65,000 computer nodes/ PCs. A total of 6961 branches have been partially computerised - with Advanced Ledger Posting Machines, Electronic Accounting Machines and Personal Computers. Of the 336 service branches, 149 had been fully computerised and 166 had been partially computerised.

The Public Sector Banks had installed 194 Automated Teller machines (ATMs) all over the country; they had issued over 8.5 lakh credit cards and over 32,000 debit cards. The latest in this area of activity has been the issue of SMART cards.

For international interconnectivity of computers and for cross-border transactions, 568 branches have been connected to the Society for Worldwide Interbank Financial Telecommunication (popularly known as S.W.I.F.T). Local Area Network of branches has been established at 571 branch locations using internal captive networks while 148 branches are on the RBINET.

The Reserve Bank has recently identified the Payment Systems area as thrust region for

computerisation in banks. The Bank has constituted a Payment Systems Advisory Committee and an operational group to make policy guidelines. The payment systems which constitute the arteries of any economy has been recognised as the focus area for this group. This group would consolidate the existing payment systems, developing new, technologically advanced modes of payments and integration of different payment and settlement systems into an efficient, integrated system that will function as a real time gross settlement (RTGS) in an on-line environment.

To facilitate these objectives, a Computer based network has also been established. This Wide Area Satellite Based network, called the Indian Financial Network (INFINET) aims at connecting computers at branches of banks. 479 branches at commercially important cities are to be connected to the INFINET in the first phase while the next phase would witness the coverage being extended to about 5000 branches.

The INFINET is a robust and secure network which would be used for effecting financial funds movements and important information flow within the country. In view of the sensitive nature of the transactions to be routed through the network and to make it totally secure, the usage of the network would be restricted to a 'Closed User Group' consisting of member banks and financial institutions only. The INFINET User Group is engaged in various aspects pertaining to the Payment Systems in the country including the issues related to security over the network, encryption and decryption of messages during transmission, standardisation of message formats, exchange of encryption keys, etc.

The Reserve Bank continues to be involved in shaping the technology vision of the banking system. Following the recommendations of the **Committee on Financial Sector Reforms**, (which is popularly known as the second Narasimham committee), a **Committee on Technology Upgradation** has been recently set up by the RBI for the Banking Sector. This committee has representation from banks, Government, technical institutions and the RBI. Among other things, this committee will look into issues relating to

(1) Encryption of Public Switching Telephone Network (PSTN) lines
(2) Admission of electronic files as evidence
(3) Record keeping
(4) Modalities for a satellite based WAN for banks and financial institutions with the necessary security systems by banks and other financial institutions, to ultimately develop a sound and an efficient payments system
(5) Methods by which technological upgradation in banks and financial institutions could be effected and in the context study the feasibility of establishment of standards, designing payments system backbone and standards relating to security levels, messages and smart cards.

Having dwelt on the various policy initiatives taken by the RBI and extent of computerisation undergone by Indian banking system, I would like to address some of the issues involved in detection and prevention of computer crimes.

Detection of Computer Crime

The threat to safe computer operations arises not only from the failure of technology to keep up with the large volume of transactions or with the failure of associated infrastructure but also come from criminal elements who manipulate the systems either for personal profit or towards destructive ends.

Computer crime is difficult to detect when it is committed by insiders, who have a good understanding of the systems and controls and are thus able to exploit the loopholes without leaving trace. Computer crime, however, is not because of illegal work of insiders alone, it has often been the handiwork of a wider spectrum of societies. School students have been known to have broken into high security systems just for pleasure. Terrorist groups and organised crime gangs have been known to attempt to sabotage critical systems to cripple economies or target large financial institutions to fund their activities. In 1993, a systems analyst in a leading UK financial institution was convicted of attempting to transfer 1.6 million pounds to criminally owned accounts abroad[5] .

Disgruntled employees target company systems to take revenge on their employers, while business rivals try to access systems to take advantage of competitors' data.

This diversity, along with the anonymity of the perpetrator who can commit such crimes from remote locations, makes the task of having profiles of criminals difficult and poses a challenge for forensic scientists and criminal investigators.

In this context, I would like to recall an incident reported by a multinational bank a couple of years back. In the reported instance, an IT expert could penetrate the multilayer password system governing the fund transfer facility of the bank, which was allowed to be self-operated by its corporate customers. He could successfully effect wire transfer of millions of dollars from a corporate account to his own / wife's account across continent to a destination in Europe. Though the corporate treasury manager of the customer was watching the fund transfer stolen and shifted before his very eyes, he was helpless in the context of such operation happening in few seconds. While the cyber reach was possible in seconds, the efforts of law enforcement took time to cross the continental legal and criminal enactment barriers to overcome before they could ultimately nab the above criminal. It is good gesture on the part of the bank to come forward to share the methodology of the above fraud with wider public through a business journal.

The above brings me to deal and stress on the aspects of legislative changes required in countries' legal frame work. I understand that one of the purposes behind organising the Seminar is to evolve and introduce relevant criminal laws covering various aspects of evidentiary and penal procedures/ practices to tackle such modern crimes involving sophisticated technologies.

Legislation and Computer Crime

With computer crime detection being a difficult task, bringing the criminals to book becomes a formidable challenge since the laws in many countries have not kept pace with technology. Laws were originally designed to protect tangible assets and may not be sufficient to guarantee the protection of electronic bits of data. It is often difficult to attribute guilt using the

existing statutes since the act of trespassing into a system and tampering with virtual data may not necessarily be specifically provided for in law. However, this point is being increasingly recognised as an area of concern and more and more countries are, therefore, enacting specific and comprehensive legislation to cover the acts of computer criminals.

Model acts passed by nations highly dependent on technology tend to provide for enhanced penalties for unlawful access to "protected computers" such as those involved in national security, banking and finance, emergency services and public utilities. Such laws also provide for penalties for unlawful access to any system, unlawful modification of computer programmes even through viruses and even to lawful abuse or misuse of computers.[6]

The Reserve Bank has for its part, made several initiatives in this regard. The framing of the model Electronic Funds Transfer (EFT) Act and rules, suggesting amendments to the various acts such as the Bankers' Book Evidence Act, the Negotiable Instruments Act, the Banking Regulation Act and the RBI Act - is in an advanced stage. The Reserve Bank is also associated with the efforts of the Ministries of Finance, Commerce and Law in the enactment of laws such as the Information Technology Act and the Cyber Laws.

Other Imperatives

The imperative to enhance the levels of computerisation in the banking industry has been strengthened by the Government's IT vision which envisages a revolution in computer penetration by the year 2010 and also by the directive recently issued by the Central Vigilance Commissioner to banks to computerise 70 per cent of banking business by January 2001. These initiatives are important since many of the deficiencies of today's operations can be traced to the outdated manual systems in place. The CVC has also desired that the listed companies should compulsorily offer the Electronic Clearing Services to their customers for payment of dividend and interest warrants. This would help avoid the risks in the existing payment modes and reduce to a great extent the incidence of non-receipt of paper-based dividend and interest warrants despatched by post and their fraudulent payment / encashment.

In future, there would be increasing focus on dematerialisation of shares and securities which would result in two advantages: first, the prevention of frauds and second, the facilitation of transactions of Government securities in an 'On-line Real Time Gross Settlement' basis.

Security Policy and the Reserve Bank's Supervisory Initiatives

All organisations which are moving towards a high level of computerisation should have in place a security policy that offers a shared vision of how controls in workplaces should be implemented with the objective of protecting location, information and eventually, the economic value of the organisation. This would need to be supplemented by education and training in these areas and reinforced by the actions and concerns of the top management so that a culture of security can be created. These controls have to be strengthened by surveillance, regular monitoring and auditing to detect unusual usage patterns and deficiencies.

These concerns have been addressed in a focussed manner at the Reserve Bank of India,

and the broad approach in this regard is, I venture to place before, worthy of attention.

In the first place, the most important point of emphasis is on prevention of crime In order to prevent computer frauds and crimes, specific computer procedures have been laid down for each activity area involving computers. These procedures detail specific requirements for

- formal controls governing physical access to computer areas in addition to physical access to computer operation on the basis of the use of passwords, valid user identification etc., and,
- technical controls for a number of operations including standardised and secure message formats, correct authentication, personal identification numbers, digital signatures, encryption and decryption of data, firewalls, and backup that would be tamper proof.

The next imperative is to conduct computer security audit. This is an activity that is gaining in importance of late and is perhaps one of the best tools available for combating computer crime. Audit of computer security -especially by professional organisations - is a vital requisite to ensure that complacency within the organisation does not result.

The broad approach outlined here cannot succeed, if there is dearth of skilled personnel. Work is, therefore, already on to groom a force of highly motivated and technically sound group of people at banks who would look after all the requirements of computerisation and also ensure that computer frauds do not occur. It is necessary that the work and operations of the group of technologically expert persons is monitored regularly by managements to ensure that crimes are not perpetuated from inside. This is a challenge since over 2 lakh personnel had also received training in the handling and concepts of computer systems in the PSBs.[7]

It is also necessary to impart sufficient skills to our bank examiners to be able to examine records effectively in computerised operating environment and also to be able to put together a picture of the operations so that they could ensure that they have access to all transactions being put through by banks. Accordingly, under a Technical Assistance project sponsored by the UK Government, the services of international consultants were utilised to impart skills to inspecting officers of the Reserve Bank. A detailed manual was also drawn up for their use.

Simultaneously, as part of the aforesaid project, guidelines were issued to the banks on the maintenance of minimum records in computerised environment so that any subsequent investigation would not be hampered by lack of understanding or lack of access to computer data. A circular on the Risks and Controls in Computers and Telecommunications was issued by the Reserve Bank to banks to help them in identifying the key risks arising out of continually growing use of computers and suggesting controls to mitigate consequential risks.

Bank Frauds in India

One input which can be of use in combating frauds consists of proper reporting of incidents of fraud. Banks are required to report to the Reserve Bank in detail the incidences of both actual and suspected frauds in banks, the progress in their resolution and the deterrent and punitive action taken in this regard. Such reports are analysed within the Reserve Bank and any aspect that the reports reveal is circulated to the banks for necessary action.

The incidence and the amounts involved in frauds in the past three years has increased with the share of large value frauds (above Rs.1 crore) being on the increase. While one may draw comfort that the efforts of the supervisors and bankers have so far been successful in containing bank frauds, it is a matter of serious concern as the growth in frauds could, if not visibly checked, encourage perpetrators to refine their tools of operation in the commission of frauds.

Our analysis of the *modus operandi* revealed that frauds so far committed has not revealed any extensive manipulation of the computer systems in the banks. However, cases have been reported where the fraud was facilitated by poor access controls. In a recently reported case, the perpetrator was able to change the borrower's limits stored in the computer by borrowing the password of the authorized personnel. This suggests that the password cannot just be treated as a friendly word. This aspect in the Indian ethos, needs to be closely looked into and the system of password determination has to be foolproof.

International Developments

The increasing dependence of banks on computer technology and the concerns arising therefrom are receiving attention from banking regulators the world over. The Basle Committee of Banking Supervisors has addressed some of the operational risks arising out of security breach of banks' computer systems and misuse of computer products in its document "Risk Management for Electronic Banking and Electronic Money Activities" (March 1998).

Having adopted computerisation at a relatively late stage of our banking development, we have the advantage of learning from the experiences of the international community and set in place corrective systems and controls in advance. In the area of emerging products, our surveillance has to be particularly strong. This is especially so in retail payment modes where the actual customers could suffer the most on account of weak security features and counterfeiting or data stealing. This is also an area where, besides supervision, regulation has to be effective and legislative sanctions have to be strongly supportive.

Conclusion

While concluding, I would like to present before this forum some of the supervisory concerns nagging me day in, day out during the discharge of my oversight responsibility on the development and expansion of IT processing capabilities both within the RBI and the banking industry in general. I would be grateful if the experts including some of the excellent IT brains from the international investigative agencies who have taken pains to come all the way for this important seminar would address them for effective IT solutions.

- With the sole focus on expansion of computerised processing, the software developers as well as the institutions concerned do not often find time for parallel development of security features. In their anxiety to put the software for regular operation within deadlines, they allow the access control and audit features to take a back seat. This needs immediate correction. Unless development of security features are also attended to at the same level of efficiency and equal speed, I am afraid that the banks will be left with beautiful software systems for public glare and access, but totally unguarded and gullible against waiting

information poachers.

- To keep up with the deadlines for Year 2000 compliance of their computer systems, the banks have gone for extensive outsourcing of software support for inventory and fixation of Y2k bugs in their existing software. Due to lack of time, most of them could have totally opened their systems in their anxiety to have a total clean up within a short time span. Unless the banks have taken steps to revise and install new access passwords and other control features, there are chances of their system remaining open to others, the danger of unauthorised access to net work systems by those skilled personnel who earlier fixed Y2k bugs of the same system is all the more real. This calls for painstaking audit of the control features of all systems which were earlier subjected to Y2k cleaning.
- I am aware the banks' internal audit wings do not possess suitable IT professionals who are skilled in a thorough computer audit function. In such a situation, the banks should without hesitation go in for EDP Audit through reputed IT Consultancy firms and such audit should be at regular periodicity, say monthly intervals and almost on the lines of concurrent audit system. In fact in multinational banks, the EDP set up consists of parallel authorities designated as System Administrator and System Auditor to oversee the operations of the processing and development wings

Today's seminar is the beginning of an effort towards addressing not only the computer related crime but also a step forward in setting up of an inter agency co-operation in this regard. The initiatives taken by Central Bureau of Investigation in this direction is laudable.

*** Inaugural address by Shri S. P. Talwar, Deputy Governor, Reserve Bank of India at the National Seminar on Computer Related Crime at New Delhi on February 24, 1999.**

1. Can be accessed at http://www.ifs.univie.ac.at
2. Quoted in Reuvid, ibid.
3. AIDP report on computer crime released at Colloquium on Computer Crimes and Other Crimes against Information Technology, held in Germany in October 1992.
4. Data taken from the Report of the Committee on Computerisation in Banks, 1989
5. Quoted in 'The Regulation and Prevention of Economic Crime', editor Jonathan Reuvid, Kogan Page, 1995.
6. The Computer Misuse Act (1992) of Singapore is one such example.
7. Data compiled from the Consolidated Statement on Progress of Computerisation in Indian Public Sector Banks for the Biannual Period ended on 30th September, 1998.