CONTENTS

ACKNOWLEDGEMENTS

- Central Bureau of Investigation
- Corporate Communication, BHEL

I T AND VIGILANCE – ACTS OR ACTIONS ?

– Amitava Chakrabarti
Manager (MSX), BHEL/PSER

The internet has fast emerged as the most effective vehicle for integrated growth of business. Every company must seriously assess its potential for using this powerful technology in management of its supply / demand chain. This enables the customers to get direct link with the information systems and they can update themselves on different information of their interest viz, production and market forecast etc. The only technical requirement is to have a PC, internet connection and browser and last but not the least a " Password ". This password is like the key of the locker wherein valued assets are stored. Valued assets in business are nothing but information and the state-of-the-art key is the " Password " . The overriding aspect of underscoring the need for password is to advocate for the security concerns. As in every sphere of life, security and protections are equally significant in the realm of Information Technology (IT) also. Growth of IT and its applications are exploding in the country. The touch of hi-tech followed by its cultural acceptance have since snowballed but not without consequences. The reach and penetration of internet may extend to well over 25 million persons in not more than two to three years time, as we would continue to observe the convergence of communication and computers as the basis of new economy.

The new generation business fundamentals are focussing more and more on speed of transmission and zero error operations. This has fostered the need for establishing practices of electronic commerce. This new concept has provided us the impetus for moving towards a paperless society. Hence, it became imperative for the country to adopt a regime of cyber laws which could determine the rights and liabilities of parties using IT for business or otherwise. United Nations Commission on International Trade Laws (UNCITRAL) had proposed a model law on electronic commerce way back in 1996. The UN General Assembly, in a resolution recommended at a later date that the states should give favourable consideration to the said model law when they enact or revise their laws. In the above mentioned scenario, the Information Technology Act 2000 was passed with the objective to grant legal recognition to electronic records, digital signatures, authentication of electronic records, retention of information, documents and records in the electronic form whenever any law required such retention for a specific period, provide for search and arrest of the accused to deter abuse of IT etc. Transactions excluded from the Act are as follows :

(i) Negotiable Instruments
(ii) Power of Attorney instructions
(iii) Trust Deeds
(iv) Wills
(v) Documents of title to immovable properties.

Information Technology Act consists of 94 Sections and 4 Schedules. These 94 sections are arranged in 13 Chapters. The 4 Schedules deal with the amendments to the Indian Penal Code, Indian Evidence Act, 1872, Bankers Book Evidence Act 1891 and Reserve Bank of India Act 1934.

While we draw our reference to Newton's third Law of Motion, the equal and opposite forces gradually started acting on the pace of progress of IT. Analysis indicates that each new development of computer technology was followed by a corresponding adaptation of crime. From the beginning of the 1950s computers were introduced in industry to control routing process. As late as twenty years after that time, the first case of computer manipulation, computer sabotage and computer espionage became known. The mass phenomenon of program piracy came along simultaneously with the spreading of personal computers in the 1980s, forcing legislation of different reform measures from 1985 onwards. Today, electronic post services, mail boxes, ISDN etc. have not only become part of general life, but also of general crime. Following examples will elaborate the concerns in an effective way :

- Large scale invoice manipulations concerning the payment of bills.
- Manipulation of account balances and balance sheets of banks.
- Misusing ATM cards either by using stolen cards or manufacturing duplicate cards.
- Sabotage by virus programs and worm programs.
- Computer Extortion of systems and data stocks.
- Hacking through telephone system, voice mail system, etc.
- Unauthorised copying and use of foreign computer programs.
- Attack on life by manipulating fight control system etc.

The internet has become the target of hackers because many companies and research communities have recently become users of the internet and are totally ignorant of the

security risks. Computers connected to the internet are vulnerable to hacking in the following ways :

1. Gopher, ftp, electronic mail or a network file system may be used to extract passwords of other vital files or to plant data that will cause a system to welcome intruders.
2. A cracker may use services that allow one computer on a network to execute programs on another computer, thereby allowing intruders to access directly.
3. Telnet, a tool for interactive communications with remote computers or Finger, a service that provides data about users, can help a cracker discover information to plan other attacks.

Under the above circumstances we can conclude that cyberspace activism is no less crucial than cross border terrorism of any kind. We can mobilise actions for preventing terrorist activities by promulgation of Preventive Legislations, Restricting Access to Critical Locations and of course by keeping constant vigil through state-of-the-art technology viz, Web Camera, Satellite Phone, VSAT and many other innovative measures with the ultimate option for battling it out. Cyberspace Activism is synonymous to Terrorism. Both are equally dangerous to the civilisation. Cyberspace Activism always adds impetus and shows way to cross border terrorism in many ways. Our policy makers have generated many Legislations to prevent and contain terrorist activities. Accordingly, it is hightime that **IT wizards should join their heads to come forward with innovative ideas to thwart P O C A (Proliferation of Cyberspace Activism) rather than passing Acts and making amendments.**

In a given situation, if the above is considered as the one side of a coin, the other side shall invariably be " Progress through Cyberspace Actions ". What is meant by this is that as long as any event stays with positives, it is " Actions "whereas "Acts " are somehow assigning a sense of negatives. Acts are implemented by enforcement but Actions are initiated spontaneously. If actions drive home with results , acts drive away from the path of progress. Unfortunately, in India , recourse to Acts has been taken more often to thwart the speed of progress. Public Sector Undertakings are also not far from such shortcomings. Need for such Acts will cease to exist on the day when we become fully conscious about the social perils and place Values first in all our efforts. Positive Vision, Mission and Values only can lead to complete metamorphosis of the system.

Eastern Region as a whole is privileged with legacy of values in the direction of Ramakrishna Paramahansa, Swami Vivekananda & Netaji Subhash Chandra Bose. Quality of thinking in this region has always been markedly different in every sphere of life. Come what may, PSER has always adhered to the positives by way of Integrity and Fairness in all matters. This is the lifeblood of PSER operations. PSER has always embarked upon transparency and has remained vigilant to the growing needs of market driven economy. **The ever agile think-tank of PSER under the astute leadership of regional head has articulated business policies with major thrust on transparency.**. Functions and processes involved with our operations have been displayed to the rest of the world thro internet. Today, everybody have got access to information in the matter of Purchase, SCT, Finance, Quality and Tendering thro internet. The role of vigilance has already taken a significant turn from " Chasing Intruders " to " Inviting Intruders " in so far as information is concerned. It is no longer a watchdog only but a roaring lion in the cyberspace also inviting attention of others. The crux of vigilance function in the present scenario must be to provide market intelligence and information on competitors and the first principle could be illustrated as follows :

V - Vision, I - Integrity, G - Goal, I - Innovation, L - Leadership, A - Achievement , N - New, C - Challenges, E - Excellence.

Let us all reaffirm our conviction on the principle of positives and pledge to advocate for its causes for effective deployment of vigilance function towards a new paradigm.

If you give enough time for self-improvement, you may not find time to criticise others.