The Challenge of Cyber Crime in India: The Role of Government

Dr. Atul Bamrara

Abstract

Nascent personal computers, high-bandwidth wireless networking technologies and the pervasive use of the internet have transformed the style of performing business. The IT infrastructure provides transmission and storage of gigantic amounts of critical information used in each domain of society and it enables government agencies to speedily interact with each other as well as with industry, citizens, state, local governments and across international boundaries. The paper focuses on an assortment of concerns related to cyber crime and the role of Government to combat the issue. Further findings draw attention to array of cyber crime which is not covered in the IT Act.

Keywords

Cyber Law, Data Diddling, Cyber Squatting, Public Key Infrastructure (PKI), Cyber Stalking

Introduction

The Internet is primarily conscientious for developing and enriching global commerce to previously implausible heights, fostering remarkable advancements in education and healthcare, and facilitating worldwide communication that was once perceived to be limited and costly (McFarlane and Bocij 2003; Jaishankar and Umasankary 2005). However, the Internet, with its immeasurable size and previously unimaginable capabilities, has a gloomy side in that it has opened windows of previously unknown criminal opportunities that not only challenge, but also transcend all physical boundaries, borders, and limitations to sense, rebuke and diminish what appears to be a growing social problem of global proportions.

The concept of cyber crime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law counterbalanced by the sanction of the state. Computer crime or cyber crime refers to any crime that involves a computer and a network (Moore 2005). The computer may have been used in the commission of a crime, or it may be the target (Kruse and Heiser 2002). Cyber Crime is criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts (techterms.com). Cyber Crime also includes non-monetary offences, such as creating and distributing viruses on other computers or posting confidential business information on the Internet. The computer may however be a target for unlawful acts in the following cases- unauthorized access to computer/ computer system/ computer networks, theft of information contained in electronic form, e-mail bombing, data diddling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

Symantec defines cyber crime as any crime that is committed using a computer or network, or hardware device. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. The crime may take place on the computer alone or in addition to other locations.

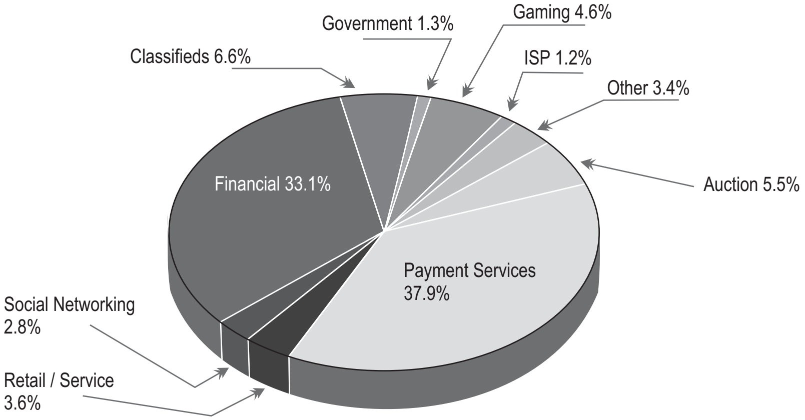
Cyber Crime Challenge

Cyber crime is the hottest and conceivably the most complicated problem in the cyber world. Industry, government and indeed society are becoming vitally dependent on IT (Anderson 1994; Apt and Olderog 1997). This dependence is illustrated by the serious concerns which are now being caused by residual Year 2000 bugs. Seeing that even these conceptually-simple software faults are demanding massive resources, we must be concerned about the much more difficult effects of cyber crimes, malicious activities by hackers or organizations seeking to exploit or disrupt an IT system, for mischief, financial gain, or more sinister motives (Benjamin 1990). Deloitte (2010) revealed a serious lack of awareness and a degree of complacency on the part of IT organizations and perhaps security officers, vis-à-vis the threat of cyber crime. Much of this belief is predicated on the notion that cyber crime technologies and techniques are so effective at eluding detection that the actual extent of the problem may be grossly underestimated. The cyber criminals constitute of various groups/ category.

Today's cyber criminals are increasingly adroit at gaining undetected access and maintaining a persistent, low-profile, long-term presence in IT environments. Meanwhile, many organizations may be leaving themselves vulnerable to cyber crime based on a false sense of security. Cyber criminals are generally computer professionals or computer-literate persons and are not history sheeters and mostly without previous criminal record (Kumar 2002). Studies also show that the threat is mostly from employees or from those with access to the system, such as maintenance personnel, hardware and software vendors, etc. However, external threats via remote access have shown an increasing trend.

The Internet is now available in over two hundred countries and because of its borderless nature. Crimes may be committed through communications that are routed through a number of different countries (U. S. Department of Justice 2000). Although cyber crimes cells have been set up in major cities of the nation but most cases of Spamming, Hacking, Phishing, Vishing remain unreported due to the lack of awareness among internet users and employees of financial institutions.

Figure 1.1 Most Targeted Industry Sectors



Source: APWG Phishing Activity Trends Report 2nd Quarter / 2010

According to APWG Phishing Activity Trends Report 2nd Quarter / 2010, Payment Services was the most targeted industry sector in Q2, as in Q1; enduring nearly 38 percent of detected attacks, up slightly from 37 percent in Q1 2010. Financial Services was second at 33 percent followed by Classifieds at 6.6 percent, though the latter exhibited the most rigorous growth of all sectors in the half. Online Classifieds emerged as a major, non-traditional Phishing sector with almost 7 percent of total Phish. The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. The internet is very fast becoming a household commodity in India. As more homes have access to internet, more children would be using the internet and more are the chances of falling victim to the aggression of paedophiles. The easy access to the pornographic contents readily and freely available over the internet lowers the inhibitions of the children.

Role of Government

A growing percentage of access is through live connections, users and organizations which are increasingly interconnected across physical and logical networks, organizational boundaries and national borders. As the framework of connectivity has broadened, the volume of electronic information exchanged in cyberspace has grown and expanded beyond traditional traffic to include multimedia data, process control signals and other forms of data. The IT infrastructure has become an integral part of the critical infrastructures of the country. The operational stability and security of critical information infrastructure is vital for economic security of the country. In addition to its underlying role in critical information infrastructures, the IT infrastructure enables large-scale processes throughout the economy, facilitating complex interactions among systems across global networks. Their interactions propel innovation in industrial design and manufacturing, e-commerce, e-governance, communications and many other economic sectors.

The IT infrastructures' significance to the country has gained visibility in the recent years due to cyber crime and rapid growth in identity theft and financial frauds. These events have made it increasingly clear that the security of the IT infrastructure has become a key strategic interest to the Government. Although the industry is now making investments in security related infrastructure, their actions are directed primarily at short-term efforts driven by market demands to address immediate security problems.

The Government has a different but equally important role to play in cyber security assurance in the form of long-term strategies. In this direction, the deliberations of the National Information Board (NIB), National Security Council (NSC) have stressed the importance of a national strategy on cyber security, development of national capabilities for ensuring ample protection of crucial information infrastructures including rapid response and remediation to security incidents. In the current environment of elevated risk created by the vulnerabilities and threats to the IT infrastructure, cyber security is not just a paperwork drill. Adversaries are capable of launching unsafe attacks on IT systems, networks, and information assets. Such attacks could damage both the IT infrastructure and other critical infrastructures. Cyber security is slowly gaining wider adoption in many consumer products for a variety of reasons. In order to highlight the growing threat to information security in India and focus related actions, Government had set up an Inter Departmental Information Security Task Force (ISTF) with National Security Council as the nodal agency. The Task Force studied and deliberated on the issues such as National information security threat perceptions, legal procedures required to ensure information security, awareness, training & research in information security, PKI infrastructure, information security policy assurance framework and nationwide information security education and awareness program. The primary objectives for securing country's cyber space are-

- Minimize damage and recovery time from cyber attacks
- Preventing cyber attacks against the country's critical infrastructures
- Reduce national vulnerability to cyber attacks
- Actions to secure cyber space include-
- Forensics and attack attribution

- Protection of networks and systems critical to national security
- Early watch and warnings
- Protection against organized attacks capable of inflicting debilitating damage to the economy
- research and technology development that will enable the critical infrastructure organizations to secure their IT assets

The Government is making efforts to identify the core services that need to be protected from electronic attacks and is seeking to work with organizations responsible for these systems so that their services are secured in a way that is proportional to the threat perception. The primary focus of these efforts is to secure the information resources belonging to Government as well as those in the critical sectors. The critical sectors include defence, finance, energy, transportation and telecommunications. Consequently, many in the industry and critical infrastructure organizations have come to recognize that their continued ability to gain consumer confidence will depend on improved software development, systems engineering practices and the adoption of strengthened security models and best practices. Cyber Security Assurance Framework aims to cater to the security assurance needs of Government and critical infrastructure organizations through enabling and endorsing actions.

Rapid identification, information exchange and remediation can often mitigate the damage caused by malicious cyberspace activity. For those activities to take place effectively at a national level, it requires a partnership between government and industry to perform analyses, issue warnings, and coordinate response efforts. The National Cyber Alert System involves public and private institutions to perform analysis, conduct watch and warning activities, enable information exchange, and facilitate restoration efforts. The essential actions under National Cyber Alert System include identification of focal points in the critical infrastructure, establish a public-private architecture for responding to national level cyber incidents, improve national incident response capabilities (CERT-In) and exercise cyber security continuity plans

CERT-In has taken steps to implement National Information Security Assurance Programme (NISAP) to create awareness in government and critical sector organisations and to develop and implement information security policy and information security best practices based on ISO/IEC 27001 for protection of their infrastructure. For communicating with these organisations, CERT-In maintains a comprehensive database of more than 1000 Point of Contacts (PoC) and Chief Information Security Officers (CISO). The technical competency of the empanelled organizations is regularly reviewed by CERT - In with the help of a test network.

CERT-In also conducted a cyber security mock drill to assess the preparedness of organizations in the critical sector to withstand cyber attacks. CERT-In plays the role of mother CERT and is regularly interacting with the cyber security officers of sectoral CERTs in defence, finance and other sectors to advise them in the matters related to cyber security.

Cyber Law and Loopholes

In the Advanced Law Lexicon dictionary, the 'Cyber law' is defined as "the field of law dealing with computers and the Internet including such issues as intellectual property rights, freedom of expression, and free access to information". The Information Technology Act 2000 was introduced on 9th June 2000. The Information Technology Act 2000 came into force on 17th October, 2000. This Act was amended vide Notification dated 27th October 2009. Mitigation that has led to the introduction of the Information Technology Act 2000 was the model law of electronic commerce known as the United Nation Commission of International Trade Law which was introduced in the general assembly of UN by its resolution No. 51 of 162 dated 30th January 1997 which has recommended that all the states should give favourable consideration to the said model law which contained equal legal treatment of user of electronic communication and paper based communication.

Business and knowledge process industries have been growing significantly during last decade in India. However, various incidents of data theft and misuse of private and personal information have raised concerns about outsourcing to India. India does not have a data protection law like US and UK. In the absence of specific legislation, data protection in India is achieved through the enforcement of privacy and property rights. Privacy rights are enforced under the Indian Constitution and the IT Act 2000, whereas the Indian Contract Act 1872, the Copyright Act 1957 and the Indian Penal Code 1860 protect property rights. The Information Technology Act deals with the hacking, tampering with computer source documents, publishing of information, which is obscene in electronic form, child pornography and breach of confidentiality & privacy, while the cyber crime other than those mentioned under the IT Act include cyber stalking, cyber squatting, data diddling, cyber defamation, Trojan attack, forgery, financial crimes, internet time theft, virus/worm attack, E-mail spoofing, Email bombing, salami attack and web jacking.

The IT Act, 2000 penalizes cyber contraventions (section 43-a to h) and cyber offences (sections 65 to 74). The former category includes gaining unauthorized access and downloading or extracting data stored in computer systems or networks. Such actions may result in civil prosecution. The latter category covers serious offences like tampering with computer source code, hacking with intent to cause changes and breach of confidentiality and privacy. Under the IT Act, a network service provider or an intermediary is liable for any known misuse of third party information or data or for not exercising due diligence to prevent the offence. Therefore, an Indian BPO company may be liable as a network service provider because it acts as a service provider and receives and transmits information or data. The IT Act covers offences and contraventions committed outside India as well, irrespective of the offender's nationality as long as the computer system or network is located in India. Confidentiality obligations are limited to officers or persons having powers under the Act and do not extend to private persons. Further, the officer is not liable to pay off the person damaged by the disclosure. Moreover, most of the penalties are in the range of two lakhs to five lakhs, which are very insignificant amounts when compared to the benefits that an individual may gain by committing crime. The Copyright Act 1957 protects Intellectual Property Rights in literary, dramatic, musical, artistic and cinematographic works. Therefore, copying a computer database or copying and distributing a database amounts to breach of copyright for which civil and criminal remedies can be initiated. However, it is difficult to make a distinction between data protection and database protection under the copyright Act. Data protection is aimed at protecting the information privacy of individuals, while database protection has an entirely different function, namely to protect of the creativity and investment put into the compilation, verification and presentation of databases. India has also witnessed cases of cyber stalking, cyber harassment and cyber defamation but as there is no precise law or provision under the IT Act. A number of cases are either not registered or are registered under the active provisions of IPC which are fruitless and do not cover the said varieties of cyber crime.

Conclusion

Law and enforcement agencies find it necessary to legalize the activities that influence our daily lives with the assistance of science. Laws are persistently being broadened and revised to defy the escalating crime rates. The Government has a diverse but equally vital role to play in cyber security assurance in the form of long-term strategies. Various initiatives have been taken by Government to combat cyber crime. CERT-In, a well quipped organization of Department of Information Technology, Ministry of Communications and Information Technology, Government of India has been established with the purpose of securing countrywide cyber space. CERT-In provides Incident Prevention and Response services as well as security quality management services. The paper focuses on various issues related to cyber crime and the role of Government to combat the issue. In the Information Technology (Amendment) Act 2008, CERT-In has been designated to serve as the National agency to execute the various functions under the umbrella of cyber security.

The author Dr. Atul Bamrara is an academic counsellor in School of Computer and Information Sciences at Indira Gandhi National Open University. His current research interests include Behavioural aspects of cyber crime and wireless telephony, Information & Communications Services in Education and E-Governance issues. His research papers have been published by reputed national and international journals of electronic commerce and information management.