CHAPTER- 4
Chapter-4

CYBER CRIME AND CYBER SECURITY: INDIAN CASES

An attempt has been made in this chapter to unfold some of the cases of cyber crime and analyzes the factors contributing to such crimes in India followed by some security devises to detect the occurrences of such crimes.

United Nations' Definition of Cyber crime:

Cyber crime spans not only state but national boundaries as well. Perhaps we should look to international organizations to provide a standard definition of the crime. At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cyber crime was broken into two categories and defined thus:

Cyber crime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

Cyber crime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network. Of course, these definitions are complicated by the fact that an act may be illegal in one nation but not in another.

These definitions, although not completely definitive, do give us a good starting point—one that has some international recognition and
agreement—for determining just what we mean by the term cyber crime. In Indian law, cyber crime has to be voluntary and willful, an act or omission that adversely affects a person or property. The IT Act provides the backbone for e-commerce and India’s approach has been to look at e-governance and e-commerce primarily from the promotional aspects looking at the vast opportunities and the need to sensitize the population to the possibilities of the information age. There is the need to take in to consideration the security aspects.

**Cyber Crime: Some Indian Case Studies:**

The Information Technology (IT) Act, 2000, specifies the acts which have been made punishable. Since the primary objective of this Act is to create an enabling environment for commercial use of I.T., certain omissions and commissions of criminals while using computers have not been included. With the legal recognition of Electronic Records and the amendments made in the several Sections of the IPC vide the IT Act, 2000, several offences having bearing on cyber-arena are also registered under the appropriate Sections of the IPC.

During the year 2003, 60 cases were registered under IT Act as compared to 70 cases during the previous year thereby reporting a decline of 14.3 percent in 2003 over 2002. Of the total 60 cases registered under IT Act 2000, around 33 percent (20 cases) relate to Obscene Publication / Transmission in electronic form, normally known as cases of cyber pornography. 17 persons were arrested for committing such offences during 2003. There were 21 cases of Hacking of computer systems wherein 18 persons were arrested in 2003. Of the total (21) Hacking cases, the cases relating to Loss/Damage of computer resource/utility under Section 66(1) of the IT Act were to the tune of 62 percent (13 cases) and that related to Hacking under Section 66(2) of IT Act were 38 percent (8 cases). During 2003, a total of 411 cases were registered under IPC Sections as compared
to 738 such cases during 2002 thereby reporting a significant decline of 44 percent in 2003 over 2002. Andhra Pradesh reported more than half of such cases (218 out of 411) (53 percent).

Of the 411 cases registered under IPC, majority of the crimes fall under 3 categories viz. Criminal Breach of Trust or Fraud (269), Forgery (89) and Counterfeiting (53). Though, these offences fall under the traditional IPC crimes, the cases had the cyber tones wherein computer, Internet or its related aspects were present in the crime and hence they were categorized as Cyber Crimes under IPC. During 2003, number of cases under Cyber Crimes relating to Counterfeiting of currency/Stamps stood at 53 wherein 118 persons were arrested during 2003. Of the 47,478 cases reported under Cheating, the Cyber Forgery (89) accounted for 0.2 per cent. Of the total Criminal Breach of Trust cases (13,432), the Cyber frauds (269) accounted for 2 percent. Of the Counterfeiting offences (2,055), Cyber Counterfeiting (53) offences accounted for 2.6 percent. A total of 475 persons were arrested in the country for Cyber Crimes under IPC during 2003. Of these, 53.6 percent offenders (255) were taken into custody for offences under Criminal Breach of Trust/Fraud (Cyber) and 21.4 percent (102) for offences under ‘Cyber Forgery’.

The age-wise profile of the arrested persons showed that 45 percent were in the age-group of 30-45 years, 28.5 percent of the offenders were in the age-group of 45-60 years and 11 offenders were aged 60 years and above. Gujarat reported 2 offenders who were below 18 years of age. Fraud/Illegal gain (120) accounted for 60 per cent of the total Cyber Crime motives reported in the country. Greed/Money (15 cases) accounted for 7.5 percent of the Cyber Crimes reported. Eve-teasing and Harassment (8 cases) accounted for around 4 per cent. Cyber Suspects include neighbours/ friends/ relatives (91), disgruntled employees (11), business competitors (9), crackers students/ professional learners (3). Cyber crime is not on the decline. The latest statistics show that cyber crime is actually on
the rise. However, it is true that in India, cyber crime is not reported too much about. Consequently there is a false sense of complacency that cyber crime does not exist and that society is safe from cyber crime. This is not the correct picture. The fact is that people in our country do not report cyber crimes for many reasons. Many do not want to face harassment by the police. There is also the fear of bad publicity in the media, which could hurt their reputation and standing in society. Also, it becomes extremely difficult to convince the police to register any cyber crime, because of lack of orientation and awareness about cyber crimes and their registration and handling by the police.

A recent survey indicates that for every 500 cyber crime incidents that take place, only 50 are reported to the police and out of that only one is actually registered. These figures indicate how difficult it is to convince the police to register a cyber crime. The establishment of cyber crime cells in different parts of the country was expected to boost cyber crime reporting and prosecution. However, these cells haven’t quite kept up with expectations. Netizens should not be under the impression that cyber crime is vanishing and they must realize that with each passing day, cyberspace becomes a more dangerous place to be in, where criminals roam freely to execute their criminals intentions encouraged by the so-called anonymity that internet provides (Singh Talwant, Addl. District & Session Judge, Delhi, Cyber Law & Information Technology).

The absolutely poor rate of cyber crime conviction in the country has also not helped the cause of regulating cyber crime. There have only been few cyber crime convictions in the whole country, which can be counted on fingers. We need to ensure that we have specialized procedures for prosecution of cyber crime cases so as to tackle them on a priority basis. This is necessary so as to win the faith of the people in the ability of the system to tackle cyber crime. We must ensure that our system provides for stringent punishment of cyber crimes and cyber criminals so that the
same acts as a deterrent for others.

**Threat Perceptions:**

UK has the largest number of infected computers in the world followed by the US and China. Financial attacks are 16 events per 1000, the highest among all kinds of attacks. The US is the leading source country for attacks but this has declined. China is second and Germany is third. It is hard to determine where the attack came from originally. The number of viruses and worm variants rose sharply to 7,360 that is a 64 per cent increase over the previous reporting period and a 332 per cent increase over the previous year. There are 17,500 variants of Win. 32 viruses. Threats to confidential information are on the rise with 54 per cent of the top 50 reporting malicious code with the potential to expose such information. Phishing messages grew to 4.5 million from 1 million between July and December, 2004.

1. **Pune Citibank Mphasis Call Center Fraud:**

US$ 3,50,000 from accounts of four US customers were dishonestly transferred to bogus accounts. This will give a lot of ammunition to those lobbying against outsourcing in US. Such cases happen all over the world but when it happens in India it is a serious matter and we cannot ignore it. It is a case of sourcing engineering. Some employees gained the confidence of the customer and obtained their PIN numbers to commit fraud. They got these under the guise of helping the customers out of difficult situations. Highest security prevails in the call centers in India as they know that they will lose their business. There was not as much of breach of security but of sourcing engineering.

The call center employees are checked when they go in and out so they cannot copy down numbers and therefore they could not have noted these down. They must have remembered these numbers, gone out immediately to a cyber café and accessed the Citibank accounts of the
customers.

All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that's how the criminals were traced. Police has been able to prove the honesty of the call center and has frozen the accounts where the money was transferred.

There is need for a strict background check of the call center executives. However, best of background checks can not eliminate the bad elements from coming in and breaching security. We must still ensure such checks when a person is hired. There is need for a national ID and a national data base where a name can be referred to. In this case preliminary investigations do not reveal that the criminals had any crime history. Customer education is very important so customers do not get taken for a ride. Most banks are guilt of not doing this.

2. Bazee.com case:

CEO of Bazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi. The Mumbai city police and the Delhi Police got into action. The CEO was later released on bail. This opened up the question as to what kind of distinction do we draw between Internet Service Provider and Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle the cyber crime cases and a lot of education is required.

3. State of Tamil Nadu Vs Suhas Katti:

The Case of Suhas Katti is notable for the fact that the conviction was achieved successfully within a relatively quick time of 7 months from the filing of the FIR. Considering that similar cases have been pending in other states for a much longer time, the efficient handling of the
case which happened to be the first case of the Chennai Cyber Crime Cell going to trial deserves a special mention.

The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the yahoo message group. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet.

On 24-3-2004 Charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC before The Hon'ble Addl. CMM Egmore by citing 18 witnesses and 34 documents and material objects. The same was taken on file in C.C. NO. 4680/2004. On the prosecution side 12 witnesses were examined and entire documents were marked as Exhibits. The Defense argued that the offending mails would have been given either by ex-husband of the complainant or the complainant herself to implicate the accused as accused alleged to have turned down the request of the complainant to marry her.

Further the Defense counsel argued that some of the documentary evidence was not sustainable under Section 65 B of the Indian Evidence Act. However, the court relied upon the expert witnesses and other evidence produced before it, including the witnesses of the Cyber Cafe owners and came to the conclusion that the crime was conclusively
proved.

Ld. Additional Chief Metropolitan Magistrate, Egmore, delivered the judgment on 5-11-04 as follows:

"The accused is found guilty of offences under Section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/- and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs. 4000/- All sentences to run concurrently."

The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered as the first case convicted under Section 67 of Information Technology Act 2000 in India.

4. The Bank NSP Case:

The Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many e-mails using the company computers. After some time the two broke up and the girl created fraudulent e-mail ids such as "Indian bar associations" and sent e-mails to the boy's foreign clients. She used the banks computer to do this. The boy’s company lost a large number of clients and took the bank to court. The bank was held liable for the e-mails sent using the bank’s system.

5. SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra

In India's first case of cyber defamation, a Court of Delhi assumed jurisdiction over a matter where a corporate reputation was being defamed through e-mails and passed an important ex-parte injunction.

In this case, the defendant Jogesh Kwatra being an employ of the plaintiff company started sending derogatory, defamatory, obscene, vulgar.
filthy and abusive e-mails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director. The plaintiff filed a suit for permanent injunction restraining the defendant from doing his illegal acts of sending derogatory e-mails to the plaintiff.

On behalf of the plaintiffs it was contended that the e-mails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature. Counsel further argued that the aim of sending the said e-mails was to malign the high reputation of the plaintiffs all over India and the world. He further contended that the acts of the defendant in sending the e-mails had resulted in invasion of legal rights of the plaintiffs. Further the defendant is under a duty not to send the aforesaid e-mails. It is pertinent to note that after the plaintiff company discovered the said employ could be indulging in the matter of sending abusive e-mails, the plaintiff terminated the services of the defendant.

After hearing detailed arguments of Counsel for Plaintiff, Delhi High Court passed an ex-parte ad interim injunction observing that a prima facie case had been made out by the plaintiff. Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive e-mails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs.

This order of Delhi High Court assumes tremendous significance as this is for the first time that an Indian Court assumes jurisdiction in a matter concerning cyber defamation and grants an ex-parte injunction restraining the defendant from defaming the plaintiffs by sending derogatory,
defamatory, abusive and obscene e-mails either to the plaintiffs or their subsidiaries.

6. Parliament attack case

Bureau of Police Research and Development at Hyderabad had handled some of the top cyber cases, including analyzing and retrieving information from the laptop recovered from terrorist, who attacked Parliament. The laptop which was seized from the two terrorists, who were gunned down when Parliament was under siege on December 13 2001, was sent to Computer Forensics Division of BPRD after computer experts at Delhi failed to trace much out of its contents. The laptop contained several evidences that confirmed of the two terrorists’ motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the three lions) were carefully scanned and the seal was also craftily made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

7. Andhra Pradesh Tax Case

Dubious tactics of a prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of computers used by the accused person. The owner of a plastics firm was arrested and Rs 22 crore cash was recovered from his house by sleuths of the Vigilance Department. They sought an explanation from him regarding the unaccounted cash within 10 days.

This case achieves clear milestones: It brings the act of “phishing” into the ambit of Indian laws even in the absence of specific legislation; It clears the misconception that there is no “damages culture” in India for violation of IP rights; This case reaffirms IP owners’ faith in the Indian
judicial system's ability and willingness to protect intangible property rights and send a strong message to IP owners that they can do business in India without sacrificing their IP rights. The Gurgaon BPO fraud has created an embarrassing situation for Infinity e-Search, the company in which Mr Karan Bahree was employed.

A British newspaper had reported that one of its undercover reporters had purchased personal information of 1,000 British customers from an Indian call-center employee. However, the employee of Infinity e-search, a New Delhi-based web designing company, who was reportedly involved in the case, has denied any wrongdoing. The company has also said that it had nothing to do with the incident.

In the immediate case the journalist used an intermediary, offered a job, requested for a presentation on a CD and later claimed that the CD contained some confidential data. The fact that the CD contained such data is itself not substantiated by the journalist.

In this sort of a situation we can only say that the journalist has used "Bribery" to induce "Out of normal behavior" of an employee. This is not observation of a fact but creating a factual incident by intervention. Investigation is still on in this matter. It later revealed that the accused was running five businesses under the guise of one company and used fake and computerized vouchers to show sales records and save tax.

8. Sony.sambandh.com case

India witnessed its first cyber crime conviction in the recent past. It all began after a complaint was filed by Sony India Private Ltd, which runs a website called www.sony-sambandh.com, targeting Non Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online.

The company undertakes to deliver the products to the concerned recipients. In May 2002, someone logged onto the website under the
identity of Barbara Campa and ordered a Sony Colour Television set and a cordless head phone. She gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim. At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

The company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code. The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company’s site.

The CBI recovered the colour television and the cordless head phone. In this matter, the CBI had evidence to prove their case and so the accused admitted his guilt. The court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code — this being the first time that a cyber crime has been convicted.

The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court therefore released the accused on probation for one year.

The judgment is of immense significance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the Indian Penal Code can be effectively applied to certain categories of cyber crimes which are not covered under the Information Technology Act.
2000. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride.

9. Nasscom vs. Ajay Sood & Others:

In a landmark judgment in the case of National Association of Software and Service Companies vs Ajay Sood & Others, delivered in March, '05, the Delhi High Court declared 'phishing' on the internet to be an illegal act, entailing an injunction and recovery of damages. Elaborating on the concept of 'phishing', in order to lay down a precedent in India, the court stated that it is a form of internet fraud where a person pretends to be a legitimate association, such as a bank or an insurance company in order to extract personal data from a customer such as access codes, passwords, etc. Personal data so collected by misrepresenting the identity of the legitimate party is commonly used for the collecting party’s advantage. Court also stated, by way of an example, that typical phishing scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details.

The Delhi HC stated that even though there is no specific legislation in India to penalize phishing, it held phishing to be an illegal act by defining it under Indian law as “his offence would go undetected but after careful scrutiny of vouchers and contents of his computers it revealed that all of them were made after the raids were conducted. Origin of the e-mail causing immense harm not only to the consumer but even to the person whose name, identity or password is misused.” The court held the act of phishing as passing off and tarnishing the plaintiff’s image. The plaintiff in this case was the National Association of Software and Service Companies

Nasscom: India’s premier software association:

The defendants were operating a placement agency involved in
head-hunting and recruitment. In order to obtain personal data, which they could use for purposes of head-hunting, the defendants composed and sent e-mails to third parties in the name of Nasscom. The high court recognized the trademark rights of the plaintiff and passed an ex-parte ad-interim injunction restraining the defendants from using the trade name or any other name deceptively similar to Nasscom. The court further restrained the defendants from holding themselves out as being associates or a part of Nasscom.

The court appointed a commission to conduct a search at the defendants’ premises. Two hard disks of the computers from which the fraudulent e-mails were sent by the defendants to various parties were taken into custody by the local commissioner appointed by the court. The offending e-mails were then downloaded from the hard disks and presented as evidence in court.

During the progress of the case, it became clear that the defendants in whose names the offending e-mails were sent were fictitious identities created by an employee on defendants’ instructions, to avoid recognition and legal action. On discovery of this fraudulent act, the fictitious names were deleted from the array of parties as defendants in the case. Subsequently, the defendants admitted their illegal acts and the parties settled the matter through the recording of a compromise in the suit proceedings. According to the terms of compromise, the defendants agreed to pay a sum of Rs. 1.6 million to the plaintiff as damages for violation of the plaintiff’s trademark rights. The court also ordered the hard disks seized from the defendants’ premises to be handed over to the plaintiff who would be the owner of the hard disks.

Undeterred by the prospect of arrest or prosecution, cyber criminals around the world lurk on the Net as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging
threat to nations' security. Headlines of cyber attacks command our attention with increasing frequency. According to the Computer Emergency Response Team Coordination Center (CERT/CC), the number of reported incidences of security breaches in the first three quarters of 2000 has risen by 54 percent over the total number of reported incidences in 1999. Moreover, countless instances of illegal access and damage around the world remain unreported, as victims fear the exposure of vulnerabilities, the potential for copycat crimes, and the loss of public confidence.

Cyber crimes-harmful acts committed from or against a computer or network-differ from most terrestrial crimes in four ways. They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.

As this report shows, the laws of most countries do not clearly prohibit cyber crimes. Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their “virtual” counterparts. Web pages such as the e-commerce sites recently hit by widespread, distributed denial of service attacks may not be covered by outdated laws as protected forms of property. New kinds of crimes can fall between the cracks, as the Philippines learned when it attempted to prosecute the perpetrator of the May 2000 Love Bug virus, which caused billions of dollars of damage worldwide.

Effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical
and legal complexities of investigating and prosecuting cyber crimes.

Six weeks after the Love Bug attack, the Philippines outlawed most computer crimes as part of a comprehensive e-commerce statute. In order to prevent a repeat of the catastrophe that prompted this action, however, the future of the networked world demands a more proactive approach, whereby governments, industry, and the public work together to devise enforceable laws that will effectively deter all but the most determined cyber criminals.

**Poor Information Security Reduces the Competitiveness of Nations**

August 2000 report, Risk e-Business: Seizing the Opportunity of Global e-Readiness, McConnell International rated mid-level economies’ capacity to participate in the digital economy. In considering nations’ information security, the report evaluated public trust in the security of information processed and stored on networks in each country. In this context, information security included: an assessment of the strength of legal protections and progress in protecting intellectual property rights, especially for software; the extent of efforts to protect electronic privacy; and the strength and effectiveness of the legal framework to authorize digital signatures. The e-Readiness report also examined the existence of legal frameworks to prosecute cyber criminals, for a predictable environment of strong deterrence for computer crime is critical to the effective protection of valuable information and networks.

Although several countries, particularly in Europe and Asia, were found to have addressed a number of these broader information security factors, few countries were able to demonstrate that adequate legal measures had been taken to ensure that perpetrators of cyber crime would be held accountable for their actions. Overall, nearly half of the countries included in the e-Readiness study were rated as needing substantial improvement in information security. In addition, only a small fraction of
countries needing substantial improvement indicated that progress was currently underway.

Outdated laws and regulations, and weak enforcement mechanisms for protecting networked information, create an inhospitable environment in which to conduct e-business within a country and across national boundaries. Inadequate legal protection of digital information can create barriers to its exchange and stunt the growth of e-commerce. As e-business expands globally, the need for strong and consistent means to protect networked information will grow.

**The Cyber Crime Laws of Nations:**

Based on its findings in the E-Readiness study, and in the wake of the Philippines inability to prosecute the student responsible for the “I Love You” virus, McConnell.

International surveyed its global network of information technology policy officials to determine the state of cyber security laws around the world. Countries were asked to provide laws that would be used to prosecute criminal acts involving both private and public sector computers.

Over fifty national governments responded with recent pieces of legislation, copies of updated statutes, draft legislation, or statements that no concrete course of action has been planned to respond to a cyber attack on the public or private sector. Countries were provided the opportunity to review the presentation of the results in draft, and this report reflects their comments.

Countries that provided legislation were evaluated to determine whether their criminal statutes had been extended into cyberspace to cover ten different types of cyber crime in four categories: data-related crimes, including interception, modification, and theft; network-related crimes, including interference and sabotage; crimes of access, including hacking and virus distribution; and associated computer-related crimes, including
aiding and abetting cyber criminals, computer fraud, and computer forgery.

Thirty-three of the countries surveyed have not yet updated their laws to address any type of cyber crime. Of the remaining countries, nine have enacted legislation to address five or fewer types of cyber crime, and ten have updated their laws to prosecute against six or more of the ten types of cyber crime.

**Law is only part of the answer:**

Extending the rule of law into cyberspace is a critical step to create a trustworthy environment for people and businesses. Because that extension remains a work in progress, organizations today must first and foremost defend their own systems and information from attack, be it from outsiders or from within. They may rely only secondarily on the deterrence that effective law enforcement can provide.

To provide this self-protection, organizations should focus on implementing cyber security plans addressing people, process, and technology issues. Organizations need to commit the resources to educate employees on security practices, develop thorough plans for the handling of sensitive data, records and transactions, and incorporate robust security technology—such as firewalls, anti-virus software, intrusion detection tools, and authentication services—throughout the organizations' computer systems.

These system protection tools—the software and hardware for defending information systems—are complex and expensive to operate. To avoid hassles and expense, system manufacturers and system operators routinely leave security features “turned off,” needlessly increasing the vulnerability of the information on the systems. Bugs and security holes with known fixes are routinely left uncorrected. Further, no agreed-upon standards exist to benchmark the quality of the tools, and no accepted methodology exists for organizations to determine how much investment in
security is enough. The inability to quantify the costs and benefits of information security investments leave security managers at a disadvantage when competing for organizational resources. Much work remains to improve management and technical solutions for information protection.

Industry-wide efforts are underway to address prevention, response, and cooperation. Around the world, various industries have been establishing information sharing and analysis centers (ISACs) to share real-time information related to threats, vulnerabilities, attacks, and countermeasures. A recent Global Information Security Summit sponsored by the World Information Technology and Services Alliance (www.witsa.org) brought together industry, governments, and multilateral organizations across economic sectors to share information and build partnerships. Post-summit working groups are now developing cooperative approaches to addressing the most critical information security problems. The results of that work will be taken up at a second summit in Belfast in May 2001. That summit will also provide an opportunity to revisit the progress of nations in updating their laws to cover cyber crimes.

Cyber crime and its implication on National security:

Global interconnectivity is making states vulnerable to new threats. Computer-based assaults or acts of information warfare, on state's systems such as nuclear establishments, energy grids, telecommunications and financial facilities could severely disrupt national defense and social services. Cyber force is a form of intervention that can produce harmful or coercive effects, and put national security at risk. It is commonly understood as structured intercepting or manipulating of industrial, military, economic and social data and information systems. Even realizing the new forms of computer-generated weapons and changing concepts of sovereignty and territory brought about by global interdependence, international law is likely to rely on UN Charter principles to define
the legal boundaries of cyberspace.

In a growing electronic economy, cyber attacks are increasingly being used for political, financial and military reasons. States or non-state units can use cyber attacks to extract critical information about strategic developments. This form of warfare can be highly anonymous and more economical given the low cost of R&D.

There are three trends that make a state or non-state enterprise transparent and vulnerable. These are, Internet enabled connectivity, Wireless networking and Mobile computing. Increasing cases of identity and data theft are becoming a major cause for concern across state and private organizations. They're causing financial loss, data loss, and loss of credibility and reputation. Critical infrastructures such as telecommunications, transportation, energy and finance can get affected by attacks on Information infrastructures. Investigations reveal that attackers are not confined to geographical boundaries.

The common targets of cyber attack include:

1. Military networks
2. Government websites
3. E-Commerce and Financial Institutions
4. Telecommunications

In 2007, Indian police acting on an intelligence lead arrested a suspected Kashmiri militant near Jalalahalli, a village north of Bangalore. Authorities confiscated an assault rifle and 300 rounds of ammunition from the suspect. Bilal Ahmed Kota, as well as - significantly - a satellite phone, a cell phone, multiple cell phone SIM cards and a map of Bangalore that marked the airport, offices of Wipro Technologies Ltd and the complex operated by Infosys Technologies. The Kota case highlighted the increase in incidents and threats to the high-tech industry, and underscores that militant groups are paying greater attention to economic target in India and
to this important sector. However, the danger of attacks by cross border militants, Maoists or Naxalites is not the only threat that corporations and state authorities now face in India. These units are confronting what is effectively a multi-pronged security threat that also includes growing concerns about personal security and kidnappings, a greater recognition of risks to intellectual property that stem from corporate espionage, and issues related to privacy and the risks of criminals stealing sensitive customer information. Security managers today have a very different perception of the risks associated with doing business in India than they a few years ago.

Significantly, dealing with each of these individual threat categories brings with it an associated business cost. As the risk environment—or perceptions of it—shift, a new question emerges: At what point will the costs of doing business in India begin to outweigh the benefits?

The demand for better methods to enforce cyber security has grown stronger since the 26/11 attacks in Mumbai. India has a dedicated organization, CERT-In, which operates under the department of communication and information technology- to tackle cyber crimes. Generating India Specific Information providing Cyber Crime, India as Target/Origin is also required for controlling cyber-crimes.

Proactive action and effective collaboration aimed at security incident prevention, prediction & protection and security assurance. However, the agency is not a prosecuting body as it does not have the legal power to examine cyber crimes.

**Cyber Security Threats:**

Organized cyber attacks have been witnessed at the Pentagon, US in June 2007, Estonia in April 2007, Computer systems of German Chancellery and three Ministries, E-mail accounts at National Informatics Centre, India and Highly classified Govt. computer networks in US, New Zealand & Australia.
A few of the Indian sites defaced by Pakistani hackers’ are:

1. Indian Science Congress
2. National Informatics Centre
3. Videsh Sanchar Nigam Limited (State-run international voice carrier)
4. External Affairs Ministry
5. Ministry of Information Technology
6. Asian Age newspaper
7. Official site of Gujarat Government
8. GlaxoWellcome India
9. Engineering Export Promotion Council, Ministry of Commerce

Few of the Pakistani sites defaced by Indian hackers are:

1. The Nation (newspaper)
2. Pakistan Television
3. Pakistan Tourism Development Corporation
4. Official site of Punjab Government
5. Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology
6. Prime bank
7. Hamdard University

Types of Cyber Weapons:

The software used to carry out these attacks indicates that they were clearly designed & tested with much greater resources. Increasing use of pen drives, CDs, mobile phones equipped with Bluetooth technologies make it difficult to keep a tab on employees and third parties. USB ports are used to connect devices like Internet data cards. While this makes it easy for state’s mobile workforce to connect to the corporate network, or use the Internet when on the move to check important mail, it also makes it easy to leak information. USB ports could be considered as a security threat. If you do plan to block all USB ports, first look for alternatives. Users are a key asset for every organization, but they're also the most vulnerable point of entry. It's easier to cajole a user into delving important
information than breaking through a firewall. This makes educating users of various security threats extremely important.

Laptop thefts are at the top of the security incidents list. Users have to be more careful and stronger focus needs to be put in training users on how to protect their laptops. Theft of confidential information could be caused by weak passwords or authentication, but they could also be caused by disgruntled employees walking away with confidential data on USB drives. The fourth one is another direct link to users-identity theft. Likewise, every user in an organization may not go through the security policy every time they want to check an e-mail or access the Internet. So there is a need to strike a balance between user expectations and an organization’s security policy. Try to remove the hazard of leaving it to the user to figure out whether the attachment in an e-mail is legitimate or not.

In early October 2009, Intelligence agencies have asked the government to consider blocking Skype as operators of the popular global VoIP (Voice over Internet Protocol) engine are refusing to share the encryption code that prevents Indian investigators from intercepting conversations of suspected terrorists. The Cabinet Committee on Security has accepted the recommendation in principle but has not set a date for initiating action. The urgency to track Skype calls stems from the fact that terrorists -- as the 26/11 attacks in Mumbai showed -- are increasingly using VoIP services. The shift to VoIP has been prompted by the growing ability of intelligence agencies to intercept mobile and other calls. Since Skype is not registered here, Indian authorities have been forced to mull the drastic option of blocking its gateways here. This, however, may not be entirely effective as Skype can route traffic through other service providers.

Need for a Legal Framework: Governments cannot control the internet in their country:

There is need for modern international law to precisely define the
criteria used to distinguish what state actions are permissible as normal computer-generated trans border data theft from those cyber activities that might qualify as an ‘armed attack’ against a state. Clearer rules are also needed for what responses are permissible as self-defense by a state targeted in an information warfare situation and how international institutions might help to attain these objectives.

Indian agencies are also keeping their fingers crossed, not sure whether the department of telecom -- with a stake in sectoral growth -- would like to lean on VoIP service providers on the issue of sharing encryption code. Besides, there's also a feeling that the government would be wary of people's response to the snapping of Skype. The free service is used by a vast majority of urban middle class Indians for communicating with families and friends spread across the world.

**Trends suggest an increase in safe havens for cyber criminals and hence the need for International cooperation arrangements.**

- It is an inevitable reality that some countries will become safe havens for cyber criminals and international pressure to crack down won't work well.

- Governments are likely to get aggressive and pursue action against the specific individuals/groups/companies, regardless of location

- It is also likely that Governments will start putting pressure on intermediary bodies that have the skills and resources, such as banks, ISPs and software vendors to protect the public from malware, hacking and social engineering.

- Compliance regulations will drive upgrades and changes and also increase system complexity and legal wrangles – increase in civil suits for security breaches.
Trained investigators:

To avoid data inaccuracies and the potential for cyber crimes, there must be a state-corporate awareness of data quality and recognition of the importance of data. There are three critical success factors that need to be identified before moving forward with the issue of data quality:

1. Commitment by senior management to the quality of corporate data
2. Definition of data quality
3. Quality assurance of data.

Senior management commitment to maintaining the quality of corporate data can be achieved by instituting a data administration department that oversees data management standards, policies, procedures, and guidelines.

The Cyber Crime Investigation Cell (CCIC) of Mumbai police arrested a former employee of a multi-national company for stealing confidential data of the firm. The company was involved in online trading of NSE and BSE stocks. With growing usage of cyber space to plan and execute actions against institutions or state, such specialized units who can gather data and convert it to actionable intelligence are more in demand.

Public Private Partnership:

In India, private security agencies investigate cyber crimes, but the Union government has not made full use of their services as in other countries. The government should seek the skills of private agencies in select cases. However, these are often sensitive issues as such cases often involve national security. We need to bridge this gap and prevent cyber threats to national security.

Industrial espionage by corporate spies in India is practiced in the information technology industries, although the KGB-trained IB and the Indian foreign intelligence service-RAW also conduct physical
surveillance of Western diplomats and high-profile Western business executives and foreign companies. Electronic eavesdropping is also practiced in India. Foreign businesses that partner with Indian firms are at risk if they do not have full control over the vetting and hiring process. Additional vulnerability comes when Indian partners outsource tasks to third-party contractors.

The risks from industrial espionage exist worldwide, but technology companies can find they are greater in India than many other regions because of the research and development (R&D) work that often is conducted there -- and because of the work of the IB and RAW, which are more aggressive than many intelligence services when it comes to stealing proprietary information from foreign companies for domestic purposes.

In addition, there have been several well-publicized cases in which Indian workers have stolen information -- such as bank account numbers, PIN numbers for automatic teller machines or birthdates and Social Security numbers (from American customers) -- for criminal purposes. For example, a worker at an Indian call centre allegedly sold the bank account information of 1,000 British customers to an undercover reporter at $7.68 per account. The call worker boasted that he was able to steal and sell up to 200,000 accounts each month.8 The Indian government is working to pass laws giving police greater enforcement powers. Employers can take steps to mitigate these risks -- but, costs are an important consideration. Monitoring employees' activities is expensive, and conducting background investigations on potential hires in a place like India can be very difficult, since public records (such as birth and death certificates) are not readily accessible or verifiable in many municipalities. Here, a public- Protecting State and Corporate Property and Investments

Increasing security risks in the environment, particularly those from targeted intrusions by experienced hackers, emphasize the
requirement to implement effective security solutions using database assurance technology. Software security solutions are now available which enable organizations to re-evaluate their systems to determine the best methods for protecting assets.

**Significant benefits of a strong cyber security management system:**

State and Corporate management needs to have a well-presented and well-documented business case, spelling out in detail the key requirements, business considerations and other elements of the proposal to obtain approval for the necessary expenditures for the selected security solution. There are significant benefits to be achieved for an organization which conducts the proper analysis and assessment of the risks and develops an appropriate security solution for database assurance, which takes account of these risks. These are the steps which have the potential for putting an organization ahead of any intrusion attempt.

A perusal of the above analysis clearly indicates that the end goal behind cyber attacks could be political, to damage the Indian economy, national interests, or revenge etc. These can be accomplished, by directly targeting the firms and state units that drive large business related investments into India. Therefore, attacks need to be viewed, reviewed and responded to intelligently.

Standard measures used by public and private corporations - such as security perimeters around office buildings, access controls and vehicle inspection points - can help to mitigate physical/terrorist threats to individual enterprises, but proactive measures to influence or change the political environment that drives the threats are necessary.

There is a need to conduct regular assessments of the security of your network. There are two key security standards exist for information security. These are BS 7799 and ISO 27000 series out of which the ISO standard seems to be more popular. India is an attractive location for
multinational IT corporations for a number of reasons. Notably, it has a large pool of highly trained, technically competent and workers who are willing to work for less pay than their counterparts in the United States or Europe. Furthermore, establishing or outsourcing customer service and support issues to call centers in India, with the time zone differences, makes it possible for companies based in the United States and Europe to offer support virtually around the clock. However, of all these reasons, the biggest motivator for multinationals to establish R&D and customer support operations in India, or to relocate those operations from other countries, has been cost. To retain this edge over other countries, Indian state and private enterprises need to successfully manage cyber threats that hamper national security. A strong public private partnership can help create an effective cyber defense.

"The system administrators and managers need to find out how to protect their computers, networks and internet sites from unauthorized intrusions. Internet users are usually uneducated about network security. Security programmes are poorly integrated. Everyday crackers & hackers brook security schemes. The United States Air force charged a small group of researchers with formidable task: treating a communication network which could survive a nuclear attack. This was a revolutionary concept: a network which had no centralized control in nutshell, this network designed exclusively for military use world survive the apocalypse itself. The individual must responsible for the internet's existence in Paul Baron. In 1962 Baron worked at Rand Corporation the think tank charged with developing this concept. Baron imagined a network where all machines could communicate with one another. This was a radical concept that went well against the gain of conventional wisdom. However, Baron knew that centralized networks were simply too vulnerable to attack (Anonymous, 1998).

In course of time, in 1969 the fine version of UNIX hardware was
developed by Ken Thompson. During the same period researchers at Dennis Ritchie and Brain Kernighan created a new programming language known as C. This language has significantly influenced the development of internet. C has some important element it is small and efficient C code is portable from one operating system to another it can be learned quickly and easily. Ray Tomlinson created internet mail in 1972, which was a significant innovation. Simple, efficient and inexpensive communication could be possible.

In 1974, Vinton Cerf and Robert Khan invented Transmission control protocol (TCP.) It was a new mechanism of moving data across the network bit by bit and then latter assembling these fragments at the other end. From 1975 onward, UNIX and the internet evolved together. Several large software and hardware manufacturers were released their own version of UNIX. Series of software companies like SUN Microsystems, Hewlett Packard, IBM, Silicon Graphics (SGI), Digital Equipment Corporation (DEC) have emerged to manufacture UNIX versions.

Installation is performed by booting from a CD –Rom. The boot routine takes quick diagnostic of all existing hardware devises checks the memory and starts vital systems process. Series of programs are available to tune up the security of a UNIX system. Security audit tools system logging tools and intrusion detection tools etc. are inbuilt in the UNIX operating system.

Internet for critical business process requires strong security devices both in processes and technology. Trained Government security personnel and increased co –ordination between Govt. agencies are pre requisite factor for internet security. National institute of standards & Technologies has a program to define standard protection profiles for security products and technologies. But there has been little effort made to move this process on internet time or to require Govt. agencies to buy products that have been
tested to these profiles. (Bansal, 2003).

Application software development and charge controls prevent unauthorized software programs or modifications to programs from being implemented. Key aspects of such controls will ensure:

- Software charges are properly authorized by the managers responsible for the agency program or operations that the application supports
- New and modified software programs are tested and approved prior to their implementation
- Approved software programs are maintained in carefully controlled libraries to protect them from unauthorized changes
- To ensure that different versions are not misidentified

Such controls can prevent errors both in software programming and malicious efforts to insert unauthorized compute program code. Without sufficient controls, incompletely tested or unapproved software will result depending on the application of such unapproved software may lead to losses or faulty outcomes.

We can also use same kind of filters to prevent mail from a known spammer and automatically transfer it to our e-mail programs electronic round file. If you log on at work server based e-mail programs such as Lotus Notes, Microsoft Exchange can be configured to block address. If you are receiving spam on the job your company’s internet administrator knows about your problem and can take measures to eradicate the same. Through filter use can block our addresses but spammers change addresses frequently. E-mail has became a vehicle for malicious hacking, much of it in the form of mail bombs. A mail bomb is simply an attack unleashed by dumping hundreds or thousands of e-mail messages on to specific addresses.
Computer viruses are bits of code that travel from computer to computer infecting each one they contact. Spam is the bane of internet e-mail: a fool used by devious marketers looking for a direct line to the minds and mailboxes of millions of buyers. Spammers buy e-mail addresses in bulk from companies that use software robots to collect them from use net posts web directories and internet access providers’ member databases. Spam costs time and money to get rid of for both internet access companies and consumers. Spam has become internet user’s big grebe. Noted companies such as America Online and Computer Server, used to sue super spammer Cyber promotions to stop its hundreds of thousands of junk messages from following their mail portals every day (Barua & Dayal, 2001).

It is not easy to get rid of the problem. There is no spam repellent that works everywhere every time. To find out unwanted mail before we notice it we need to use a buzo filter. Most e-mail programs have built in filters routing mail to different in boxes storing messages based on their importance and blocking mail from stalkers odd and others.

Cyber Security Case Studies; Case Study: 1

A provider of online prescriptions recently experienced a security breach where account information was stolen out of the company’s database, including patient’s social security numbers. You have been hired as a consultant to conduct a thorough analysis of the information system in order to develop recommendations for improved security. You need to develop a thorough understanding of the existing system, and of which security tools, security measures and intrusion detection systems are currently in place. You also need to gain knowledge of which internal and external “users” of the information system have access to what information, what level of privilege they hold, and why they need the information and what they do with it. The research process will involve examining detailed
technical specifications and system administration procedures, interviewing users of the system, reviewing security procedures and information flow diagrams. As part of the proposed solution, you will run scenarios to test system vulnerabilities. You will need to educate yourself on the regulations that are pertinent to the management of information in the context of online pharmacies.

Recommendations will most likely include technical upgrade to the system, revisions of information access protocols and upgrade to user authentication. It may include training of company personnel at all levels of the organization. You may recommend improved system maintenance and regular security tests of the system for vulnerabilities. Some of these solutions may require significant investment of money and time and you will need to clearly show the necessities of these investments against the potential cost of non-compliance.

Case Study: 2

You are a trainer for information assurance in a government organization. You are very knowledgeable about the different regulation relating to information assurance in government organizations, and keep current with all the changes and new regulations. You also understand information assurance best practices and are able to adapt them to specific government organizations and units. You have the ability to convert operating procedures to training guidelines and use instructional design principles and tools very effectively. Your technical knowledge is thorough enough to answer general technical questions from your audience but you are not a technical expert and will refer detailed questions to technical support staff.

In preparation for each training session, you gather and analyze information relevant to specified information assurance policies and requirements of your audience, and write plans and procedural materials for
the expansion of the existing policies and requirements. You maintain records tracking the sources of information collected and versions of training materials produced. You often work with subject matter experts (SMEs) in order to refine your presentation and better adapt it to your audience. You rely on excellent communication skills (both written and verbal) and solid organization skills.

Case Study: 3

You work for a financial institution. You are part of a team that provides reporting on information assurance and cyber security procedures from your organization to regulatory agencies. The reports include system security plans, contingency plans, privacy procedures and impact assessments, and tracking plan of action and milestones. When any system change is planned or implemented, your team is involved to assess the security impact from such changes. You are involved in the testing of new system releases and in the monitoring of existing systems and security procedures. You provide recommendations at all stages of system design, implementation and maintenance to ensure that the system continues to be compliant with relevant information assurance and cyber security regulations. Even though your team is not directly responsible for developing and communicating security policies to company personnel, you review these policies in great detail and are called upon to recommend improvements. You also provide support during the system certification phase and recommendations to the management on how to maintain the security accreditation of the system.

You will continuously keep abreast of changes in security threats, best practices, regulations and compliance and translate these changes in terms that the technical group, user group and management can apply to their operations and planning.
Cyber Law Cases in India and World

Myspace catches a murderer:

My Space has played an important role in helping Oakland police apprehend a 19-year old man accused of shooting a San Leandro High School football player Greg "Doody" Ballard, Jr. Oakland police had a street name of a suspect and were able to identify Dwayne Stancil, 19 of Oakland from a picture they found on a gang's My Space page. Police brought the suspect to their headquarters where detectives say he confessed. What was most troubling to investigators was the lack of motive for the killing. We can cite an extract of the news related to cyber crime in the following paragraph:

OFFICIAL WEBSITE OF MAHARASTRA GOVERNMENT HACKED:

MUMBAI, 20 September 2007 - IT experts were trying yesterday to restore the official website of the government of Maharashtra, which was hacked in the early hours of Tuesday. Rakesh Maria, joint commissioner of police, said that the state’s IT officials lodged a formal complaint with the Cyber Crime Branch police on Tuesday. He added that the hackers would be tracked down. Yesterday the website, http://www.maharashtragovernment.in, remained blocked. Deputy Chief Minister and Home Minister confirmed that the Maharashtra government website had been hacked. He added that the state government would seek the help of IT and the Cyber Crime Branch to investigate the hacking. “Serious view has been taken of this hacking, and if need be the government would even go further and seek the help of private IT experts. Discussions are in progress between the officials of the IT Department and experts,” Patil added.

The state government website contains detailed information about government departments, circulars, reports, and several other topics. IT
experts working on restoring the website told Arab News that they fear that the hackers may have destroyed all of the website’s contents. According to sources, the hackers may be from Washington. IT experts said that the hackers had identified themselves as “Hackers Cool Al-Jazeera” and claimed they were based in Saudi Arabia. They added that this might be a red herring to throw investigators off their trail. According to a senior official from the state government’s IT department, the official website has been affected by viruses on several occasions in the past, but was never hacked. The official added that the website had no firewall.

Three people held guilty in online credit card scam

Customers’ credit card details were misused through online means for booking air-tickets. These culprits were caught by the city Cyber Crime Investigation Cell in Pune. It is found that details misused were belonging to 100 people.

ICICI Prudential Life Insurance officer had complained on behalf of one of his customer. In this regard Mr. Sanjeet Mahavir Singh Lukkad, Dharmendra Bhika Kale and Ahmead Sikandar Shaikh were arrested. Lukkad being employed at a private institution, Kale was his friend. Shaikh was employed in one of the branches of State Bank of India.

According to the information provided by the police, one of the customers received a SMS based alert for purchasing the ticket even when the credit card was being held by him. Customer was alert and came to know something was fishy; he enquired and came to know about the misuse. He contacted the Bank in this regards. Police observed involvement of many Banks in this reference.

The tickets were book through online means. Police requested for the log details and got the information of the Private Institution. Investigation revealed that the details were obtained from State Bank of India. Shaikh was working in the credit card department; due to this he had
access to credit card details of some customers. He gave that information to Kale. Kale in return passed this information to his friend Lukkad. Using the information obtained from Kale Lukkad booked tickets. He used to sell these tickets to customers and get money for the same. He had given few tickets to various other institutions.

    Cyber Cell head DCP Sunil Pulhari and PI Mohan Mohadikar A.P.I Kate were involved in eight days of investigation and finally caught the culprits. In this regards various Banks have been contacted; also four airline industries were contacted. DCP Sunil Pulhari has requested customers who have fallen in to this trap to inform police authorities on 2612-4452 or 2612-3346 if they have any problems.

How cyber crime operations work – and why they make money

    Hackers are no longer motivated by notoriety – it's now all about the money. Guillaume Lovet, Threat Response Team Leader at security firm Fortinet, identifies the players, their roles and the returns they enjoy on their investments. Cyber crime which is regulated by Internet Law (Cyber Law) or IT Act has become a profession and the demographic of your typical cyber criminal is changing rapidly, from bedroom-bound geek to the type of organized gangster more traditionally associated with drug-trafficking, extortion and money laundering. It has become possible for people with comparatively low technical skills to steal thousands of pounds a day without leaving their homes. In fact, to make more money than can be made selling heroin (and with far less risk), the only time the criminal need leave his PC is to collect his cash. Sometimes they don't even need to do that. In all industries, efficient business models depend upon horizontal separation of production processes, professional services, sales channels etc. (each requiring specialized skills and resources), as well as a good deal of trade at prices set by the market forces of supply and demand.

    Cyber crime is no different: it boasts a buoyant international market
for skills, tools and finished product. It even has its own currency. The rise of cyber crime is inextricably linked to the ubiquity of credit card transactions and online bank accounts. Get hold of this financial data and not only can you steal silently, but also – through a process of virus-driven automation – with ruthlessly efficient and hypothetically infinite frequency. The question of how to obtain credit card/bank account data can be answered by a selection of methods each involving their own relative combinations of risk, expense and skill. The most straightforward is to buy the ‘finished product’. In this case we’ll use the example of an online bank account. The product takes the form of information necessary to gain authorized control over a bank account with a six-figure balance. The cost to obtain this information is $400 (cyber criminals always deal in dollars). It seems like a small figure, but for the work involved and the risk incurred it’s very easy money for the criminal who can provide it. We need to note that this is an international trade; many cyber-criminals of this ilk are from poor countries in Eastern Europe, South America or South-East Asia. The probable marketplace for this transaction will be a hidden IRC (Internet Relay Chat) chartroom. The $400 fee will most likely be exchanged in some form of virtual currency such as e-gold. Not all cyber-criminals operate at the coalface, and certainly don’t work exclusively of one another; different protagonists in the crime community perform a range of important, specialized functions.

These broadly encompass:

Coders – comparative veterans of the hacking community:

With a few years' experience at the art and a list of established contacts, ‘coders’ produce ready-to-use tools (i.e. Trojans, mailers, custom bots) or services (such as making a binary code undetectable to AV engines) to the cyber crime labour force – the ‘kids’. Coders can make a few hundred dollars for every criminal activity they engage in. Kids – so-
called because of their tender age: most are under 18. They buy, trade and resell the elementary building blocks of effective cyber-scams such as spam lists, php mailers, proxies, credit card numbers, hacked hosts, scam pages etc. ‘Kids’ will make less than $100 a month, largely because of the frequency of being ‘ripped off’ by one another. Drops – the individuals who convert the ‘virtual money’ obtained in cyber crime into real cash. Usually located in countries with lax e-crime laws (Bolivia, Indonesia and Malaysia are currently very popular), they represent ‘safe’ addresses for goods purchased with stolen financial details to be sent, or else ‘safe’ legitimate bank accounts for money to be transferred into illegally, and paid out of legitimately. Mobs- professionally operating criminal organizations combining or utilizing all of the functions covered by the above. Organised crime makes particularly good use of safe ‘drops’, as well as recruiting accomplished ‘coders’ onto their payrolls. Gaining control of a bank account is increasingly accomplished through phishing. There are other cyber crime techniques, but space does not allow their full explanation. All of the following phishing tools can be acquired very cheaply: a scam letter and scam page in your chosen language, a fresh spam list, a selection of php mailers to spam-out 100,000 mails for six hours, a hacked website for hosting the scam page for a few days, and finally a stolen but valid credit card with which to register a domain name. With all this taken care of, the total costs for sending out 100,000 phishing e-mails can be as little as $60. This kind of ‘phishing trip’ will uncover at least 20 bank accounts of varying cash balances, giving a ‘market value’ of $200 – $2,000 in e-gold if the details were simply sold to another cyber criminal. The worst-case scenario is a 300per cent return on the investment, but it could be ten times that.

Better returns can be accomplished by using ‘drops’ to cash the money. The risks are high, though: drops may take as much as 50per cent of the value of the account as commission, and instances of ‘ripping off’ or
‘grassing up’ to the police are not uncommon. Cautious phishers often separate themselves from the physical cashing of their spoils via a series of ‘drops’ that do not know one another. However, even taking into account the 50 per cent commission, and a 50 per cent ‘rip-off’ rate, if we assume a single stolen balance of $10,000 – $100,000, then the Phisher is still looking at a return of between 40 and 400 times the meager outlay of his/her phishing trip.

In large operations, offshore accounts are invariably used to accumulate the criminal spoils. This is more complicated and far more expensive, but ultimately safer.

The alarming efficiency of cyber crime can be illustrated starkly by comparing it to the illegal narcotics business. One is faster, less detectable, more profitable (generating a return around 400 times higher than the outlay) and primarily non-violent. The other takes months or years to set-up or realizes an investment, is cracked down upon by all almost all governments internationally, fraught with expensive overheads, and extremely dangerous.

Add phishing to the other cyber-criminal activities driven by hacking and virus technologies – such as carding, adware/spyware planting, online extortion, industrial spying and mobile phone dialers – and you’ll find a healthy community of cottage industries and international organizations working together productively and trading for impressive profits. Of course these people are threatening businesses and individuals with devastating loss, financial hardship and troubling uncertainty – and must be stopped.

On top of viruses, worms, bots and Trojan attacks, organizations in particular are contending with social engineering deception and traffic masquerading as legitimate applications on the network. In a reactive approach to this onslaught, companies have been layering their networks
with stand alone firewalls, intrusion prevention devices, anti-virus and anti-spyware solutions in a desperate attempt to plug holes in the armory. They're beginning to recognize it's a failed strategy. After all, billions of pounds are being spent on security technology, and yet security breaches continue to rise.

To fight cyber crime there needs to be a tightening of international digital legislation and of cross-border law enforcement co-ordination. But there has been need to be a more creative and inventive response from the organizations under threat. Piecemeal, reactive security solutions are giving way to strategically deployed multi-threat security systems. Instead of having to install, manage and maintain disparate devices, organizations can consolidate their security capabilities into a commonly managed appliance. These measures combined, in addition to greater user education are the best safeguard against the deviousness and pure innovation of cyber-criminal activities.

Technology nuances are important in a spam infested environment where privacy can be compromised and individuals can be subjected to become a victim unsuspectingly. We need to sensitize our investigators and judges to the nuances of the system. Most cyber criminals have a counter part in the real world. If loss of property or persons is caused the criminal is punishable under the IPC also. Since the law enforcement agencies find it is easier to handle it under the IPC, IT Act cases are not getting reported and when reported are not necessarily dealt with under the IT Act. A lengthy and intensive process of learning is required.

A whole series of initiatives of cyber forensics were undertaken and cyber law procedures resulted out of it. This is an area where learning takes place every day as we are all beginners in this area. We are looking for solutions faster than the problems can get invented. We need to move faster than the criminals.
The real issue is how to prevent cyber crime. For this, there is need to raise the probability of apprehension and conviction. India has a law on evidence that considers admissibility, authenticity, accuracy, and completeness to convince the judiciary. The challenge in cyber crime cases includes getting evidence that will stand scrutiny in a foreign court.

In the present global situation where cyber control mechanisms are important we need to push cyber laws. Cyber Crimes are a new class of crimes to India rapidly expanding due to extensive use of internet. Getting the right lead and making the right interpretation are very important in solving a cyber crime. The system cannot be stronger than the weakest link in the chain. In India, there are 30 million policemen to train apart from 12,000 strong Judiciary. Police in India are trying to become cyber crime savvy and hiring people who are trained in the area. Each police station in Delhi will have a computer soon which will be connected to the Head Quarter. The pace of the investigations however can be faster; judicial sensitivity and knowledge need to improve. Focus needs to be on educating the police and district judiciary. IT Institutions can also play a role in this area.

For this India needs total international cooperation with specialized agencies of different countries. Police has to ensure that they have seized exactly what was there at the scene of crime, is the same that has been analyzed and the report presented in court is based on this evidence. It has to maintain the chain of custody. The threat is not from the intelligence of criminals but from our ignorance and the will to fight it. The law is stricter now on producing evidence especially where electronic documents are concerned. The computer is the target and the tool for the perpetration of crime. It is used for the communication of the criminal activity such as the injection of a virus/worm which can crash entire networks.

The growing danger from crimes committed against computers, or
against information on computers, is beginning to claim attention in national capitals. In most countries around the world, however, existing laws are likely to be unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information.

Self-protection, while essential, is not sufficient to make cyberspace a safe place to conduct business. The rule of law must also be enforced. Countries where legal protections are inadequate will become increasingly less able to compete in the new economy. As cyber crime increasingly breaches national borders, nations perceived as havens run the risk of having their electronic messages blocked by the network. National governments should examine their current statutes to determine whether they are sufficient to combat the kinds of crimes discussed in this report. Where gaps exist, governments should draw on best practices from other countries and work closely with industry to enact enforceable legal protections against these new crimes.

**Concluding remarks and suggestions:**

1. Reliance on terrestrial laws is an untested approach. Despite the progress being made in many countries, most countries still rely on standard terrestrial law to prosecute cyber crimes. The majority of countries are relying on archaic statutes that predate the birth of cyberspace and have not yet been tested in court.

2. Weak penalties limit deterrence. The weak penalties in most updated criminal statutes provide limited deterrence for crimes that can have large-scale economic and social effects.

3. Self-protection remains the first line of defense. The general weakness of statutes increases the importance of private sector efforts to develop and adopt strong and efficient technical solutions and management
practices for information security.

4. A global patchwork of laws creates little certainty. Little consensus exists among countries regarding exactly which crimes need to be legislated against. Figure 2 illustrates the kinds of gaps that remain, even in the 19 countries that have already taken steps to address cyber crimes. In the networked world, no island is an island. Unless crimes are defined in a similar manner across jurisdictions, coordinated efforts by law enforcement officials to combat cyber crime will be complicated.

5. A model approach is needed. Most countries, particularly those in the developing world, are seeking a model to follow. These countries recognize the importance of outlawing malicious computer-related acts in a timely manner in order to promote a secure environment for e-commerce. But few have the legal and technical resources necessary to address the complexities of adapting terrestrial criminal statutes to cyberspace. A coordinated, public-private partnership to produce a model approach can help eliminate the potential danger from the inadvertent creation of cyber crime havens.

In the light of the above analysis the following measures are forwarded in order to prevent the occurrence of cyber crime and to minimize its incidence. The weak state of global legal protections against cyber crime suggests three kinds of action.

1. **Firms should secure their networked information.**

   Laws to enforce property rights work only when property owners take reasonable steps to protect their property in the first place. As one observer has noted, if homeowners failed to buy locks for their front doors, should towns solve the problem by passing more laws or hiring more police? Even where laws are adequate, firms dependent on the network must make their own information and systems secure. And where
enforceable laws are months or years away, as in most countries, this responsibility is even more significant.

2. Governments should assure that their laws apply to cyber crimes.

National governments remain the dominant authority for regulating criminal behavior in most places in the world. One nation already has struggled from, and ultimately improved, its legal authority after a confrontation with the unique challenges presented by cyber crime. It is crucial that other nations profit from this lesson, and examine their current laws to discern whether they are composed in a technologically neutral manner that would not exclude the prosecution of cyber criminals. In many cases, nations will find that current laws ought to be updated. Enactment of enforceable computer crime laws that also respect the rights of individuals are an essential next step in the battle against this emerging threat.

3. Firms, governments, and civil society should work cooperatively to strengthen legal frameworks for cyber security.

To be prosecuted across a border, an act must be a crime in each jurisdiction. Thus, while local legal traditions must be respected, nations must define cyber crimes in a similar manner. An important effort to craft a model approach is underway in the Council of Europe (see www.coe.int), comprising 41 countries. The Council is crafting an international Convention on Cyber Crime. The Convention addresses illegal access, illegal interception, data interference, system interference, computer-related forgery, computer-related fraud, and the aiding and abetting of these crimes. It also addresses investigational matters related to jurisdiction, extradition, the interception of communications, and the production and preservation of data. Finally, it promotes cooperation among law enforcement officials across national borders.

Late in its process, the Council began to consider the views of affected industry and civil society. This process is making the Council's
product more realistic, practical, efficient, balanced, and respectful of due process that protects individual rights. At this point, most observers support provisions to improve law enforcement cooperation across borders. However, industry, through the World Information Technology and Services Alliance (see www.witsa.org/press/), argues that the requirements on service providers to monitor communications and to provide assistance to investigators, as outlined in the Draft Convention, would be unduly burdensome and expensive. Another provision considered objectionable could criminalize the creation and use of intrusive software, or hacking programs, which are designed for legitimate security testing purposes. This action could stifle the advances in technology vital to keep up with evolving cyber threats. Privacy and human rights advocates (see www.gilc.org) object to the Draft Convention’s lack of procedural safeguards and due process to protect the rights of individuals, and to the possibility that the ensuing national laws would effectively place restrictions on privacy, anonymity, and encryption.

The Council plans to release a final draft of the Convention in December 2000. In 2001, a political process involving national governments will determine the scope and coverage of the final Convention. Because of cyber crime’s international potential, all countries, and all companies, are affected. Interested parties, including national governments from outside Europe, and businesses and non-governmental organizations from around the world, should participate vigorously in a consensus process to develop measures that support effective international law enforcement and foster continued growth and innovation.

Cyber-cafe or the presence of internet facilities can aid development and improve standard of living. The services of cybercafé are very important in nation building. Useful educational materials, research and economic information are brought closer to users there by reducing unnecessary tension and making work easy to accomplish at much reduced
time and cost.

**Conclusion:**

It is deduced from the analysis that the internet services provide a common meeting place for people. It brings the world closer and serves a melting pot of ideas. It becomes a market place for users as business are transacted in the net, contracts are being sort for, and even employment opportunities are found. In the present day, admissions and scholarship into colleges and universities are easily facilitated in the net. Correspondences are changing hands as interaction between/among people who have never met before interact on the net. More interesting is the fact that it opens up a social connection for people of the same and different ages, sexes and provides solutions to nagging problems that could have taken so many years to solve if the net services were not available. Thus to be cut off from internet facilities is a bad signal of being cut off from progress and development. The most disturbing thing about the cyber café/internet facilities is that a new wave of crime has been introduced into the system. This is known as internet crime or cyber crime. Cyber crime is one of the fastest growing criminal activities on the planet. It covers a wide range of illegal activities. Crime is one of the fastest growing criminal activities on the planet. It covers a wide range of illegal activities. Longe and Chiemeke (2008) expressed that cyber crimes remain elusive and ever strive to hide itself in the face of development.

It goes without saying that it is perplexing and disturbing these days to find that print out are falsified, certificates are forged, banks are robbed, and individuals are thrown into financial and moral bankruptcy because of the nefarious activities people perpetrate on the net. Criminal activities of any kind is inimical to progress and development; be it social, economic and educational. Cyber crime could be worse than armed robbery due to the intricacy of its operations.
McConnell International (MI) is a global technology policy and management consulting firm that helps clients seize opportunities in the new economy. Its proven approach of using trusted public and private networks to leverage the risk of e-business and e-government gives clients a unique advantage. MI currently manages the United Nations-sponsored global cooperation network of government Internet policy officials from over 120 countries.

1. See www.cert.org. Although the following organizations also track reported incidents, global statistics have yet to be compiled: the National Infrastructure Protection Center (NIPC), www.nipc.gov, the Computer Security Institute (CSI), www.gocsi.com, and the Internet Fraud Complaint Center, www.ifccfbi.gov.

2. Victims of recent attacks include: Yahoo, CNN Interactive, Amazon.com, eBay, Datek Online, E*Trade, ZDNet, and Buy.com.


4. The countries evaluated are: Albania, Australia, Brazil, Bulgaria, Burundi, Canada, Chile, China, Cuba, the Czech Republic, Denmark, Dominican Republic, Egypt, Estonia, Ethiopia, Fiji, France, Gambia, Hungary, Iceland, India, Iran, Italy, Japan, Jordan, Kazakhstan, Latvia, Lebanon, Lesotho, Malaysia, Malta, Mauritius, Moldova, Morocco, New Zealand, Nicaragua, Nigeria, Norway, Peru, Philippines, Poland, Romania, South Africa, Spain, Sudan, Turkey, United Kingdom, United States, Vietnam, Yugoslavia, Zambia, and Zimbabwe.

5. In March 2005, when a police raid in New Delhi turned up evidence of plans for attacks against IT companies in Bangalore, many private security companies and security directors for multinational corporations
assumed the threat was being exaggerated by the Indian press. In March 2006: The police presence around high-tech businesses in Hyderabad was increased, and authorities called for companies to review their security measures, after Indian authorities said they had received what they characterized as a credible threat against customer service and support centers in that city. Source: Fred Burton, “Corporate Security: Risk and Cost Tolerance in India,” Jan 10 2007, http://www.stratfor.com/corporate_security_risk_and_cost_tolerance_india. SPAM – India specific data.

