E-SECURITY ISSUES

Mani Arora
Lecturer in Department of Commerce and Management
Hindu Kanya College, Kapurthala

Abstract:

With the rapid growth of e-commerce, governmental and corporate agencies are taking extra precautions when it comes to protecting information. The development of e-security as a discipline has enabled organisations to discover a wider array of similarities between attacks occurring across their security environment and develop appropriate countermeasures. To further improve the security of information, there is a need for conceptualising the interrelationships between e-security and the major elements involved in changing a company's infrastructure. Organisations should act in an ethical manner, especially when it comes to e-security and e-privacy policies, procedures, and practices. The consequential theory of utilitarianism is used and applied to a conceptual model to help explain how organisations may develop better secured information in an information-sharing and globally networked environment.

E-security is a critical concern for both consumers and business. Establishing trust between all parties in an online transaction is vital for the success of e-commerce. The public wants full assurance that the information they supply is going to the company they think it is going to, will not be misused by that company, and that credit card information or other payment mechanisms are confidential and secure. On the other hand, companies also want that their systems must remain protected from intruders and they cannot tamper with the data. Some degree of risk is always associated with E-transactions, if security controls are not applied while engaging into such transactions. Users must be sure before engaging into transactions that they are safe and the information provided by them is not going to unauthorized people.

Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

In this paper, I have covered the e-security issues such as elements of e-security, security threats or cyber crimes, tools for e-security, precautions for secure e-commerce and various studies regarding e-security issues.

Index: Introduction, Meaning, Cyber Crime Types of Cyber Crimes, Basic Principles of E-Security, Top 10 E-Security Tips, Cyber Crime Statistics

Introduction

The Internet, which is the network of networks, is the primary medium for conducting e-business. Internet technology enables the world to become interconnected. The world of internet is an open public network which is open to all any time anywhere in the world. The data can be exposed to the whole world. Internet offers great opportunities to many industries, such as financial, telecommunications, health, transportation, etc. Since the original purpose of the internet was not for commercial purposes, it is not designed to handle secure transactions. People using internet are, for one or other transaction concerned about safety of their transactions. Surveys show that lack of transaction security is one of the key reasons why consumers are hesitant about shopping online. Surveys show that consumers are reluctant to make their transactions online because of security concerns. These security concerns stem from a number of factors. The principal cause of security concern has to do with the key innate characteristics of the internet as an open system. Heinous crimes such as theft, fraud and extortion can occur in great magnitude within a matter of seconds. Cyber crimes are growing at alarming rate not only in advanced countries but also in developing countries.

E-Security is a thought leader within the information security paradigm, and collects and analyses a wide range of strategic data.

E-Security is able to provide advice on issues of trust and identity for transactions within the Internet environment. Specifically, the use of Web 2.0 functionality to provide a basis for building e-commerce relationships, enhancing reputation and establishing a better cultural understanding with customers and stakeholders.

E-Security is available to provide impartial and vendor-neutral research tailored for industry sectors.

Meaning

E-security or Electronic security means the security mechanisms or aspects related to E-commerce. E-security can be defined as **the use of 'adequate precautions' to protect the user's data and systems.** It is the adoption of certain measures which safeguard user's crucial data from unauthorized use.

E-security is a critical concern for both consumers and business. Establishing trust between all parties in an online transaction is vital for the success of e-commerce. The public wants full assurance that the information they supply is going to the company they think it is going to, will not be misused by that company, and that credit card information or other payment mechanisms are confidential and secure. On the other hand, companies also want that their systems must remain protected from intruders and they cannot tamper with the data. When examining internet security or when considering the purchase of any internet security system, there are a few basic factors to consider:

- What information, processes, records and communications need to be protected ?
- What are the potential threats and risks that the threats will occur ?
- How the security system will interact with other applications currently in use ?
- What are the potential strengths and limitations of security options ?

- What other equipment (hardware or software) will be needed to make it secure as possible ?
- What type of training will employees need to ensure that the system functions properly ?

Ansewering these questions will help to identify specific internet security needs while assessing the strengths and limitations of e-security tools that are being considered. Once an understanding of e-security needs is established, the appropriate solutions can be selected.

Cyber Crime

Some degree of risk is always associated with E-transactions, if security controls are not applied while engaging into such transactions. Users must be sure before engaging into transactions that they are safe and the information provided by them is not going to unauthorized people.

In Simple way we can say that cyber crime is unlawful act wherein the computer is either a tool or a target or both.

Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

We can categorize Cyber crimes in two ways :
The Computer as a Target :-using a computer to attack other computers e.g. Hacking, Virus/Worm attacks, DOS attack etc.

The computer as a weapon :-using a computer to commit real world crimes e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Cyber Crime regulated by Cyber Laws or Internet Laws.

Technical Aspects

Technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies such as

- **Unauthorized Access & Hacking:-**

Access means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.

Unauthorized access would therefore mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network.

Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money.

- **Trojan Attack:-**

The program that act like something useful but do the things that are quiet damping. The programs of this kind are called as Trojans. The name Trojan Horse is popular.

Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the trojan.

- **Virus and Worm attack:-**

A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus.

Programs that multiply like viruses but spread from computer to computer are called as worms.

- **E-mail related crimes:-**

1. Email spoofing

Email spoofing refers to email that appears to have been originated from one source when it was actually sent from another source.

2. Email Spamming

Email "spamming" refers to sending email to thousands and thousands of users - similar to a chain letter.

3.Sending malicious codes through email

E-mails are used to send viruses, Trojans etc through emails as an attachment or by sending a link of website which on visiting downloads malicious code.

4. Email bombing

E-mail "bombing" is characterized by abusers repeatedly sending an identical email message to a particular address.

5. Sending threatening emails

6. Defamatory emails

7. Email frauds

- **Denial of Service attacks(DOS):-**

A distributed denial of service (DoS) attack is accomplished by using the Internet to break into computers and using them to attack a network.

Hundreds or thousands of computer systems across the Internet can be turned into “zombies” and used to attack another system or website.

Types of DOS

There are three basic types of attack:

a. Consumption of scarce, limited, or non-renewable resources like NW bandwith, RAM, CPU time. Even power, cool air, or water can affect.

b. Destruction or Alteration of Configuration Information

c. Physical Destruction or Alteration of Network Components

- **Money Laundering:-**:

This is form of white color crime. The internet provides the companies and individuals with the opportunity of marketing their products on the internet. It is also easy for people in

concealing the origin of ill-gotten gains. Electronic money laundering is increasing day by day. Under electronic money laundering one can conceal the gain in such transaction which is liable to tax. Tax evasion is also possible because legitimately derived income can be concealed easily and tax could be saved by this method.

- **Pornography:-**

The literal meaning of the term 'Pornography' is "describing or showing sexual acts in order to cause sexual excitement through books, films, etc."

This would include pornographic websites; pornographic material produced using computers and use of internet to download and transmit pornographic videos, pictures, photos, writings etc.

Adult entertainment is largest industry on internet.There are more than 420 million individual pornographic webpages today.

Research shows that 50% of the web-sites containing potentially illegal contents relating to child abuse were 'Pay-Per-View'. This indicates that abusive images of children over Internet have been highly commercialized.

Pornography delivered over mobile phones is now a burgeoning business, "driven by the increase in sophisticated services that deliver video clips and streaming video, in addition to text and images."

- **Forgery:-**

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. Also impersonate another person is considered forgery.

- **IPR Violations:-**

These include software piracy, copyright infringement, trademarks violations, theft of computer source code, patent violations. etc.

Cyber Squatting- Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under trademark laws.Cyber Squatters registers domain name identical to popular service provider's domain so as to attract their users and get benefit from it.

- **Cyber Terrorism:-**

Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc.

Cyberterrorism is an attractive option for modern terrorists for several reasons.

1.It is cheaper than traditional terrorist methods.

2.Cyberterrorism is more anonymous than traditional terrorist methods.

3.The variety and number of targets are enormous.

4.Cyberterrorism can be conducted remotely, a feature that isespecially appealing to terrorists.

5.Cyberterrorism has the potential to affect directly a larger number of people.

- **Banking/Credit card Related crimes:-**

In the corporate world, Internet hackers are continually looking for opportunities to compromise a company's security in order to gain access to confidential banking and financial information. Use of stolen card information or fake credit/debit cards are common.Bank employee can grab money using programs to deduce small amount of money from all customer accounts and adding it to own account also called as salami.

- **E-commerce/ Investment Frauds:-**

Sales and Investment frauds. An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered.

The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site.Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

- **Sale of illegal articles:-**

This would include trade of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication. Research shows that number of people employed in this criminal area. Daily peoples receiving so many emails with offer of banned or illegal products for sale.

- **Online gambling:-**

There are millions of websites hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

- **Defamation: -**

Defamation can be understood as the intentional infringement of another person's right to his good name. Cyber Defamation occurs when defamation takes place with the help of computers and / or the Internet, e.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends. Information posted to a bulletin board can be accessed by anyone. This means that anyone can place Cyber defamation is also called as Cyber smearing.

- **Cyber Stacking:-**

Cyber stacking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc. In general, the harasser intends to cause emotional distress and has no legitimate purpose to his communications.

- **Pedophiles:-**

Also there are persons who intentionally prey upon children. Specially with a teen they will let the teen know that fully understand the feelings towards adult and in particular teen parents. They earns teens trust and gradually seduce them into sexual or indecent acts.Pedophiles lure the children by

distributing pornographic material, then they try to meet them for sex or to take their nude photographs including their engagement in sexual positions.

- **IdentityTheft:-**

Identity theft is the fastest growing crime in countries like America. Identity theft occurs when someone appropriates another's personal information without their knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes.

- **Data diddling:-**

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file.It also include automatic changing the financial information for some time before processing and then restoring original information.

- **Theft of Internet Hours:-**

Unauthorized use of Internet hours paid for by another person. By gaining access to an organisation's telephone switchboard (PBX) individuals or criminal organizations can obtain access to dial-in/dial-out circuits and then make their own calls or sell call time to third parties.

Additional forms of service theft include capturing 'calling card' details and on-selling calls charged to the calling card account, and counterfeiting or illicit reprogramming of stored value telephone cards.

- **Theft of computer system (Hardware):-**

This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

- **Physically damaging a computer system:-**

Physically damaging a computer or its peripheralseither by shock, fire or excess electric supply etc.

- **Breach Privacy and Confidentiality:-**

Privacy or confidentiality is important for all sensitive data such as credit card numbers, social security numbers, government files, etc. information should be out of reach of unauthorized internal users, external hackers and it could not be intercepted during the course of transmission of communication.

Basic Principles of E-Security

A business has to consider the security of information while it is being transmitted and while it is being stored on computer and networks. Following are basic principles of e-security:

- ✓ **Privacy**

Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others. Breach of privacy means unauthorized use or distribution or disclosure of personal information like medical records, sexual preferences, financial status etc.

- ✓ **Confidentiality**

It means non disclosure of information to unauthorized or unwanted persons. In addition to Personal information some other type of information which useful for business and leakage of such information to other persons may cause damage to business or person, such information should be protected.

Generally for protecting secrecy of such information, parties while sharing information forms an agreement about the procedure of handling of information and to not to disclose such information to third parties or use it in such a way that it will be disclosed to third parties.

Many times party or their employees leak such valuable information for monitory gains and causes breach of contract of confidentiality.

Techniques/tools of privacy and confidentiality:

1. **Encryption**: Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. The use of encryption/decryption is as old as the art of communication. In wartime, a cipher, often incorrectly called a code, can be employed to keep the enemy from obtaining the contents of transmissions. (Technically, a code is a means of representing a signal without the intent of keeping it secret; examples are Morse code and ASCII.) Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals.

In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that undoes the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to break the cipher. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on the communications without access to the key.

Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to tap than their hard-wired counterparts. Nevertheless, encryption/decryption is a good idea when carrying out any kind of sensitive transaction, such as a credit-card purchase online, or the discussion of a company secret between different departments in the organization. The stronger the cipher -- that is, the harder it is for unauthorized people to break it -- the better, in general. However, as the strength of encryption/decryption increases, so does the cost.

In recent years, a controversy has arisen over so-called strong encryption. This refers to ciphers that are essentially unbreakable without the decryption keys. While most companies and their customers view it as a means of keeping secrets and minimizing fraud, some governments view strong encryption as a potential vehicle by which terrorists might evade authorities. These governments, including that of the United States, want to set up a key-escrow arrangement. This means everyone who uses a cipher would be required to provide the government with a copy of the key. Decryption

keys would be stored in a supposedly secure place, used only by authorities, and used only if backed up by a court order. Opponents of this scheme argue that criminals could hack into the key-escrow database and illegally obtain, steal, or alter the keys. Supporters claim that while this is a possibility, implementing the key escrow scheme would be better than doing nothing to prevent criminals from freely using encryption/decryption.

2.**Firewall:** A **firewall** is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices which is configured to permit or deny computer applications based upon a set of rules and other criteria.

Firewalls can be implemented in either hardware or software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

Packet filter: Packet filtering inspects each packet passing through the network and accepts or rejects it based on user-defined rules. Although difficult to configure, it is fairly effective and mostly transparent to its users. It is susceptible to IP spoofing.

Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.

Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

- ✓ **Authenticity:** authentication is a mechanism to verify that message senders are who they are. The receiver of the transaction or any message can be confident of the identity of the sender or the integrity of the message. When a message is received, it should be possible to verify whether it has been sent by a person claiming to be the originator and recipient of data.
- ✓ **Integrity:** Integrity of message means that their contents remain unmodified during the course of transmission. The message should appear exactly as it was stored or sent. Information must not be accidently altered or destroyed. It must be clear that no one has added, deleted or modified any part of the message. If it has been done so it should be possible to generate an alert on any modification, addition or deletion to original contents.

Techniques of Data Integrity:

1. **Digital Signatures:** A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

Assume you were going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you.

1. You copy-and-paste the contract (it's a short one!) into an e-mail note.
2. Using special software, you obtain a message hash (mathematical summary) of the contract.
3. You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash.
4. The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.)

At the other end, your lawyer receives the message.

1. To make sure it's intact and from you, your lawyer makes a hash of the received message.
2. Your lawyer then uses your public key to decrypt the message hash or summary.
3. If the hashes match, the received message is valid.

2. **Anti VirusSoftwares:** Anti Virus Software is packaged with most computers and can counter most virus threats if the software is regularly updated and correctly maintained. With thousands of new viruses being generated every month, it is essential that the virus database to be kept up to date. The virus database is the record held by the antivirus package that helps it to identify known viruses when they attempt to strike.
   - ✓ **Access control:** Access control means we are giving permission or denying the permission for a particular thing. When the access of electronic documents is given to authorized users, it is accessing those resources and when we do not give permission or access, that means, access is not given, it is controlled. A business house must keep its resources secure, so that only the authorized persons can have access to data and unauthorized persons do not.

   Techniques of Access Control:

   1. **Web Filtering Software:** Web Filtering Software is used to screen and exclude from access or availability of web pages

that are deemed objectionable or non-business related. Web Filtering is used by corporations, schools, universities and home computer owners.

2. **Intrusion Detection:**Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment (sometimes refered to as scanning), which is a technology developed to assess the security of a computer system or network.

Intrusion detection functions include:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

✓ **Data availability:**Data availability states that information stored or transported must be available to the desired user under any *condition.*

Top 10 E-Security Tips

1. Develop a 'culture of security'
Businesses need to have Internet security measures in place and make sure staff are aware of, and follow, Internet security practices.

2. Install anti-virus software and keep it updated
Anti-virus software scans and removes known viruses your computer may have contracted. It will help protect your computer against viruses, worms and Trojans.

3. Install a firewall to stop unauthorised access to your computer
Firewalls work like a security guard to protect your computer from intruders.

4. Protect yourself from harmful emails
Be cautious about opening emails from unknown or questionable sources.

5. Minimise spam
While it is not possible to completely stop spam from entering your email box, you can take steps to reduce the amount.

6. Back-up your data
Creating a copy of back-up of data is a sensible way to ensure that you can recover all of your business information from your computer or website quickly and easily.

7. Develop a system for secure passwords
Creating effective passwords can provide an additional means of protecting the information on your computer.

8. Keep your software up-to-date
If your software is out of date, you are more vulnerable.

9. Make sure your online banking is secure
If you bank online you should follow security advice provided by your financial institution.

10. Develop and maintain a security policy
You need to monitor and test security polcies.

Cyber Crime Statistics

The following cyber crime statistics illustrate of some of the general trends in the field of hi-tech crimes. Marked increases in cyber crime statistics result in an increasing need for professionals capable of responding to and investigating cyber crimes, and conducting Cyber Crime Statistics from the 2006 Internet Crime Report. The Internet Crime Complaint Center is a clearinghouse for online economic crime complaints. It is maintained by the National White Collar Crime Center and the Federal Bureau of Investigations. Highlights are as under:

• In 2006, the Internet Crime Complaint Center received and processed over 2,00,000complaints.

• More than 86,000 of these complaints were processed and referred to various local,state, and federal law enforcement agencies.

• Most of these were consumers and persons filing as private persons.

• Total alleged dollar losses were more than $194 million.

• Email and websites were the two primary mechanisms for fraud.

• Although the total number of complaints decreased by approximately 7,000 complaintsfrom 2005, the total dollar losses increased by $15 million.

• The top frauds reported were auction fraud, non-delivery of items, cheque fraud, andcredit card fraud.

• Top contact mechanisms for perpetrators to victims were email (74%), web page(36%), and phone (18%) (there was some overlap).

Cyber Crime Statistics from the 12th Annual Computer Crime andSecurity Survey

This survey is conducted annually by the Computer Security Institute.Interestingly, these statistics are compiled from voluntary responses of computersecurity professionals. Thus, there is certainly an inference that the damages due tocomputer security incidents are much higher than those cited here, as companies withoutresponding security professionals undoubtedly were the victim of computer securityincidents. Highlights are as under:

• Between 2006 and 2007 there was a net increase in IT budget spent on security.

• Significantly, however, the percentage of IT budget spent on security awarenesstraining was very low, with 71% of

respondents saying less than 5% of the securitybudget was spent on awareness training, 22% saying less than 1% was spent onsuch training.

• 71% of respondents said their company has no external insurance to covercomputer security incident losses.

• 90% of respondents said their company experienced a computer security incidentin the past 12 months.

• 64% of losses were due to the actions of insiders at the company.The top 3 types of attack, ranked by dollar losses, were:

• financial fraud ($21.1 million)

• viruses/worms/trojans ($8.4 million)

• system penetration by outsiders ($6.8 million)

UCR National Incident Based Reporting System

The UCR National Incident Based Reporting System (NIBRS) collects incident andarrest-level crime data maintained in law enforcement records (similar to Canada's UCR2survey). The NIBRS includes a category that captures data oncomputer crime incidents.

In 2000, of the 45,950 computer crimes reported by the NIBRS. 5,744 were crimes wherethe computer was the tool and 40,211 were crimes where the computer was the object.

Table 1

Computer Crime Offences by Type, 2000, United States

Computer was:	**Tool**	**Object**
Assault Offences	878	282
Sex offences, forcible	73	15
Kidnapping/Abduction	12	32
Sex offences, non-forcible	5	0
Murder & Non-negligent Manslaughter	0	1
Crimes Against the Person	968	330
Drug/Narcotic Offences	605	606
Weapon Law violations	36	52
Pornography/Obscene Material	108	1
Gambling offences	6	4
Prostitution Offences	9	0
Crimes Against Society	764	663
Larceny/Theft Offences	1,589	19,950
Destruction/Damage/Vandalism of Property	485	2,990
Burglary/Breaking and Entering	373	14,174
Fraud Offences	756	595
Counterfeiting/Forgery	525	293
Motor Vehicle Theft	110	386
Embezzlement	84	277
Robbery	37	220
Stolen Property Offence	31	283
Arson	10	39
Extortion/Blackmail	7	10
Bribery	5	1
Crimes Against Property	4,012	39,218
Total	**5,744**	**40,211**

69 agencies submitted data where an offender was suspected of using computer equipment to commit a crime. 102 agencies submitted data where computer hardware/software was the object of the crime in 2000. The NIBRS represents 13% of

police agencies in the United States accounting for 16% of the US population.

Source: National Incident Based Reported System, Federal Bureau of Investigation, U.S. Department of Justice.

Bibliography

- *NitiSoni, Dr. RuchiTrehan, Fundamentals of E-Business.*
- *Sarkaria, Rai and Sardana, Fundamentals of E-Business*
- *Philip Kotler, Markaeting.*
- *www.google.com*
- *www.yahoo.com*