International Journal of Electronics Engineering, 4 (2), 2012, pp. 193–197

Security Risk Management with Networked Information System: A Review

Puja Gupta[1] and Rakesh Kumar[2]

[1]Research Scholar, [2]Supervisor NIMS University Rajasthan, Jaipur, India

Abstract: The paper presents various issues related to cyber crimes and their detection mechanisms. The detailed analysis of issues related with cyber crimes committed through networks is presented.

Keywords: Cyber Crimes, Hacking, Network Security.

1. INTRODUCTION

Nonprofits aren't Immune to "Network Security", Computers are making crime easier at nonprofit organizations. Network security is a branch of technology known as information security as applied to computers and networks. The term computer system security means the collective processes and mechanism by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individual and unplanned activities respectively. The strategies & methodologies of computer security often differ from most other computer technologies because of its somewhat elusive objective of unwanted computer behavior instead of enabling wanted computer behavior.

Network information acts as "acts punishable by the information technology Act". It's an evil having its origin in growing dependence on computer in modern life. In this age, everything from microwave ovens, refrigerators to nuclear power plants are being run on computers. It has assumed rather sinister implication. Major problems regarding network security in the recent past include Citibank rip of USA $10 million were fraudulently transferred out of the bank account in Switzerland. A Russian hacker group led by Vladimir Kevin, a renowned hacker perpetrated the attack. The group comprised the bank's security system Vladimir used, computer firm in St. Petersburg, Russia to break into Citibank computer. He was finally arrested.

1.1. Computer Crimes

The speed and efficiency that benefit the organization serve the criminal equally well. Computer ability to transform financial data into speedy, invisible systems has made it easier for criminals to hide their thefts for longer periods.

While there is a sophisticated reporting system for violent crimes, there is nothing comparable for computer crimes (defined as crimes in which perpetrators use a computer as a tool). Although there are few statistics, it is clear that the problem is growing. Studies show that loss from fraud and embezzlement is about 10 times higher when a computer is used than when it isn't. The speed and efficiency that benefit the organization serve the criminal equally well. Further, information housed in computerized systems is invisible. Criminals can conceal data manipulation more easily when review is available only through system access.

The combination of speed and invisibility allows perpetrators to steal more over a longer period of time than ever before. Moreover, many incidents aren't reported for fear of bad press, and many perpetrators are never caught. One investigator was "struck by the incompetence of most of the embezzlers who were discovered. One can't help but wonder what the really clever people are doing." **Computer crime**, or **cybercrime**, refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. **Net crime** refers to criminal exploitation of internet. Such crimes may threaten a nation's security and financial health. Issues surrounding this type of crime have become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare. The international legal system is attempting to hold actors accountable for their actions through the International Criminal Court.

1.2. Types of Computer Crimes

One category of computer crime includes age-old types of crime, such as embezzlement and fraud, with the computer as a new accomplice. A second category introduces a

completely new set of crimes unique to the widespread use of computers. This second category includes:

- Unauthorized access, modification, copying, and destruction of software or data;
- Theft of computer time;
- Theft or destruction of hardware;
- Use or conspiracy to use computer resources to commit a felony; and
- Intent to illegally obtain information or property through use of the computer.

Literature available on such study is very scanty and however some workers have given certain guidelines in this direction. In India for other crimes a large amount of work is available through various agencies and Government department and other. However on net crime no such documented work on the issue is presently available. To fill the gap in this knowledge in this prime an area, in depth study has been referred with the specific objective on the identification of various types of cyber crime and their documentation and to suggest ways and means to reduce cyber crime in various sectors.

2. LITERATURE REVIEW

Some of the relevant literature reviews are discussed here:

Allen, B., (1977) "The Biggest Computer Frauds Lessons for CPAs," Journal of Accountancy, 1977, 143(5). A sobering reality is that most computer crimes are discovered by chance. Not all nonprofits perform regular audits. Even if they do, audits don't always uncover the criminal activity. An early study of computer crimes 9 lists these ways that computer crimes were detected: A bank employee suspected the embezzlement. An error was made by the perpetrator when he became too greedy. During the yearly audit, auditors detected an inventory shortage. A wife reported her husband's suspicious activity. An IRS investigation uncovered fraud. A police raid revealed gambling activities by an employee, and further investigation turned up massive embezzlement. A fellow employee became suspicious. A bank messenger failed to deliver checks on time. The perpetrator was absent because of illness, and her replacement discovered the criminal activity.

Official Website of Maharashtra 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.

Griffith, (1990) The) Computer) Fraud) and) Abuse) Act) of) (1986): A measured) Response) to) A) Growing) Problem,) 43) Vanderbilt for criminal) law) from) time) to) time) whenever) a) new) type) of) harmful) conducts) emerges.) This) was although emergence extent.

Report of (1993) is that the Nation on Occupational Fraud and Abuse prepared by the Association of Certified Fraud Examiners (ACFE). Such cases are all too common. Not only can the loss of money devastate a nonprofit, but the incident can cause a loss of public confidence, leading to reduced contributions.

UTI Bank hooked up in a Phishing Attack Fraudsters of cyberspace have reared its ugly head, the first of its kind this year, by launching a phishing attack on the website of Ahmadabad-based UTI Bank, a leading private bank promoted by India' s largest financial institution, Unit Trust of India (UTI).

Indian Websites are new target of Hackers Some computer experts managed to break into the high security computer network of Bhabha Atomic Research Center but were luckily detected.

Online Credit Card Fraud on E-Bay Bhubaneswar: Rourkela police busted a racket involving an online fraud worth Rs 12.5 lakh. The modus operandi of the accused was to hack into the eBay India website and make purchases in the names of credit cardholders.

Orkut a danger a social networking site led their users in danger as Abhishek a teenager played a prank by accusing a fake account by name of a girl and this landed him into jail.

3. RESEARCH METHODOLOGY

The present study is be based on secondary source of information and all the relevant data, literature, documents, books, published reports, newspaper, journals, different agencies involved in computer crimes and investigating agencies were consulted for necessary data input on the subject of the study to meet desired objective as stated above.

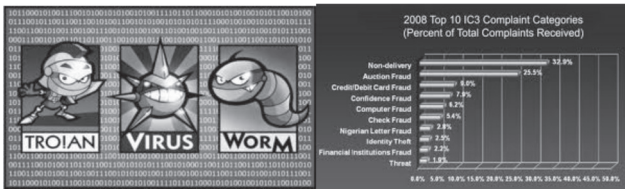
3.1. Discussion

On the basis of the information on the different aspects of cyber crime the information generated has been analyzed properly and discussed in the following paragraph. 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.

3.2. Cyber Crime can be Categorized in Two Ways

The Computer as a Target:-using a computer to attack other computers. Such as Hacking, Virus/Worm attacks. The computer as a weapon:-using a computer to commit real world crimes. e.g. Cyber Terrorism, Credit card frauds, Cyber stacking etc.

Unauthorized access & Hacking means to access any kind of access without the permission of the person in charge of a computer, computer system or computer network.



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 to commit financial crimes 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: This program means to do something useful but do the things harmful the most common name given is Trojan horse. It comes in two parts i.e.

1. Client part
2. Server part

Virus and Worm: This program has the capability of infecting the other programs by making multiple copies of itself and spreading it into other program. These viruses are sent from one computer to another through e-mail. By sending E-Mail to thousands and thousands of users similar to the chain letter that means Email Spamming. Emails are used to send viruses and Trojan by sending some website links and by visiting/downloading the same website may cause deliberately harmful.

Banking/Credit card Related crimes: Internet hackers continuously keep on looking for the opportunity for gaining the confidential and financial information as it is most common that a bank employee/hacker may deduce desired amount of money from all customer's account and transferring it to own account also called as salami.

E-commerce/ Investment Frauds: These are sales and investment frauds i.e. the dealing done online for the purchase of any article will not be 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. Fraudulent promises the high profits schemes that are not fulfilled.

Cyber Stacking: Cyber Stacking involves following the person movement across the Internet by posting the messages i.e. threatening messages to the victim constantly bombarding the victim through e-mails. In general it results into harassment that causes emotional distress.

Phishing: "Phishing" is the act of attempting to fraudulently acquire sensitive information, such as passwords and credit card details, masked as a trustworthy person or business with a real need for such information in a seemingly official electronic notification or message (most often an email, or an instant message). It is a form of social engineering attack.

3.3. Places that Effected due to Cyber Crime

Official Website of Maharastra Government Hacked: http://www.maharashtragovernment.in, remained blocked. As IT expert tried restoring the website of Maharashtra which was hacked in the early hours of Tuesday. According to the IT Experts, hackers are from Washington and they identified themselves as "Hackers Cool Al-Jazeera" and claimed they were based in Saudi Arabia. The expert also quoted that the official website has been affected broadly by the viruses on several occasions in the past, but was never hacked. The official added that the website had no firewall.

3.4. UTI Bank Hooked Up in a Phishing Attack

Fraudsters of cyberspace have reared its ugly head, by launching a phishing attack on the website of Ahmadabad-based UTI Bank, a leading private bank promoted by India's largest financial institution, Unit Trust of India (UTI). The tricky link is available on *http://br.geocities* By Phishing the fraudster created the web pages of the UTI Bank which asks the customer their personal details including their username and password and all account details which led to crime. The bank has sent alerts to all its customers informing about such malicious websites, besides beefing up their alert and fraud response system. Top Officials have reported the case to Delhi police. After investigation, it was found that Mail form is a service of PC Svet, which is a part of the Czech company PES Consulting. The Webmaster of the site is a person named Petr Stastny whose e-mail can be found on the web page.

Some computer experts managed to break into the high security computer network of Bhabha Atomic Research Center but were luckily detected.

The NAASCOM chief said Indian companies on an average spent only 0.8 per cent of their technology budgets on security, against a global average of 5.5 per cent.

CBI Director said a number of cases of hacking of Indian internet sites have been traced to Pakistan but it would be difficult to nail them. Hackers using knowledge of software to break in and steal information from computer systems broke into at least 635 Indian internet sites last year.

3.5. Online Credit Card Fraud on E-Bay

Rourkela police tracked a racket online fraud of Rs. 12.5 lakh. The technique was to hack into the eBay India website and make purchases in the names of credit cardholders. Two persons, including alleged mastermind Culprit, a BCA

student, were arrested and forwarded to the court of the sub divisional judicial magistrate, Rourkela. Culprit's allegedly hacked into the eBay India site and gathered the details of around 700 credit cardholders. They then made purchases by using their passwords. The fraud came to the notice of eBay officials when it was detected that several purchases were made from Rourkela while the customers were based in cities such as Bangalore, Baroda and Jaipur and even London, said deputy manager of eBay. The company brought the matter to the notice of Rourkela police after some customers lodged complaints. The Culprit used the address of other person for delivery of the purchased goods, said police. The gang was involved in train, flight and hotel reservations.

3.6. ORKUT: The New Danger

"Orkut, the online entry purchased by Google finds itself a center of debate. A nineteen-year-old student has been accused of making a fake account of a girl. Can we prevent the misuse of this technology by not posting our numbers and pictures? ABHISHEK NEVER IMAGINED that the prank he played on his classmate would land him in jail. Abhishek, a management student and still in his teens, was arrested by the Thane police following a girl's complaint about tarnishing her image in the public forum–Orkut."

3.7. How to Report Cyber Crime to Police?

Filing a complaint/Writing an application letter. The complainant may need to provide the following possible information, along with an application letter addressing the head of cyber crime investigation cell when filing a complaint: The name, mailing address, telephone number, Specific details on how the offence was committed, along with the names and addresses of suspects and any other relevant information necessary**.**

3.8. Cyber Stalking

It is the most common kind of cyber crime happening in India and the victim's report could contain the following information: Email/IM communications received, Phone numbers of the obscene callers, if any, Website address which contains the profile, Screenshot or the webpage (to be saved and submitted in hard copy), Other important necessary information could be provided after consulting law enforcement agency.

Password Hacking: When did you access your email account last?, From where and which computer did you browse it?, All information about email account e.g. date of birth entered, pin code entered and security question and the last password?

Documents to be included as proof or evidence in regard to the complaint?: Every possible information which can be provided by applicant with proper documents can be included in the application letter and be considered as proof or evidence.

Proof or Evidence may include the following:-E-mail printouts, Chat-room or newsgroup text or screenshots if taken by complainant, Email printouts should contain full email header information, Transaction acknowledgements or receipts, Credit card records, transaction details and receipts, Envelopes or letters received via post courier, FAX copies, Pamphlets or brochures (if you have received), Phone bills, Printed or preferably electronic copies of web pages, Keep the necessary information in a safe location; you will be required to provide them for investigation as and when required. Proof or documents which will be part of the application are not restricted to the above list; additional information may be required depending on the nature of crime.

Children: Children should not give out identifying information such as Name, Home address, School Name or Telephone Number in a chat room. They should not give photographs to anyone on the Net without first checking or informing parents' guardians. They should not respond to messages, which are suggestive, obscene, belligerent or threatening, and not to arrange a face-to –face meeting without telling parents or guardians. They should remember that people online might not be who they seem.

General Information: Don't delete harmful communications (emails, chats etc). They will provide vital information about system and address of the person behind these. Try not to panic. If you feel any immediate physical danger contacts your local police. Avoid getting into huge arguments online during chat and discussions with other users. Remember that all other Internet users are strangers; you do not know who you are chatting with. So be careful. Be extremely careful about how you share personal information about yourself online. Choose your chatting nickname carefully so as others. Do not share personal information in public space online; do not give it to strangers. Be extremely cautious about meeting online introduced person. If you choose to meet, do so in a public place along with a friend. If a situation online becomes hostile, log off and if a situation places you in fear, contact local police. Save all communications for evidence. Do not edit it in any way. Also, keep a record of your contacts and inform Law Enforcement Officials.

Preventive Steps For Organisations And Government:

- Physical security
- Access control
- Password
- Finding the holes in network
- Using network scanning programs
- Using encryption
- Detection.

4. CONCLUSION

The study has been found to be very useful and valuable in the detection of various kinds of cyber crimes. It is

interesting to note that "The NAASCOM chief said Indian companies on an average spent only 0.8 per cent of their technology budgets on security, against a global average of 5.5 per cent.

CBI Director said a number of cases of hacking of Indian internet sites have been traced to Pakistan but it would be difficult to nail them. Hackers using knowledge of software to break in and steal information from computer systems broke into at least 635 Indian internet sites last year." The author has tried to analyze in detail various issues related with cyber crime committed through network and since it is an exploratory study more attention and work is suggested in this direction in its entirety.

REFERENCES

[1] Criminal Investigation Department Review, January 2 (MIS Cyber Crime Scenario in India Criminal Investigation Department.

[2] Criminal Investigation Department Review January 18, 2008 Chandigarh Tribune, Monday, May Review January 19, 2008

[3] Criminal Investigation Department Review, 28, 2001 January 19, 2008.

[4] Criminal Investigation Department Review 18, 2008, January 20, 2008 *Amar Ujala*, Oct. 10, 2008 *Dainik Jagran*, April 17.

[5] *Dainik Jagran*, Dec. 14, 2009 *Dainik Jagran*, Dec. 18, 2009 *Dainik Jagran*, Feb. 5, 2010 *Dainik Jagran*, May 7, 2010.

[6] *Dainik Jagran*, Nov. 18, 2009 *Dainik Jagran*, Dec. 5 , 2009 *Dainik Jagran*, Dec. 19, 2009 *Dainik Jagran*, May 8, 2010 *Economic Times* Crime Survey, 2006 *Express India.com,* Sunday, Oct. 28 , 2007, *The Business Line* Monday , July 23, 2007 *The Hindu*.

[7] *The Hindu Business Line*, Tuesday, Jul. 31, 2007, Jan. 5, 2006 *The Hindu* Sunday, Nov 26, 2006, *The Hindu* Wednesday, Jan 17, 2007.

[8] *www.womensissues.about.com*

[9] *www.cert.org*

[10] *www.cybercellmumbai.com*

[11] *www.cyberlaws.net*

[12] *www.gohacking.com*