2011 3rd International Conference on Information and Financial Engineering
IPEDR vol.12 (2011) © (2011) IACSIT Press, Singapore

Technical management issues for resolving the cyber crime

Ajeet Singh Poonia[#1], Dr. G. S. Dangayach[*2], Dr. Awadesh Bhardwaj[*3],

[#1] Department of Computer Science and Engineering
College of Engineering and Technology, Bikaner, India.
pooniaji@gmail.com
[*2] Department of Mechanical Engineering
[*3] Department of Management Studies
* Malviya National Institute of Technology, Jaipur, India.
[2] dangayach@gmail.com
[3]awbh2001@gmail.com

Abstract. With the exponential growth of computers inhabiting the earth with many millions of miles of optical fiber, wire and air waves, link people, their computers and the vast array of information handling devices together, we can say that we are living in cyber era. As we know that each and everything in the world has its own pros and cons, so has the Cyber system. This exponential growth, and the increase in its capacity and accessibility coupled with the decrease in cost, has brought about revolutionary changes in every aspect of human civilization, including crime. The new breed of crime, which is either penetrated using computers, or is otherwise related to them, is broadly termed as Cyber crime. This cyber crime is coming in new forms embedded with new technologies, which is very difficult to investigate with the available resources. To stand with them we need a hi-tech technology enabled security system and investigators along with the awareness among the common man, as today's crime have no defined boundaries.

Keywords：cyber world, cyber society, cyber system, cyber crime.

1. Introduction

Cyber means virtual and in the field of Information System it play a major role i.e. the thing exist but you cant get it real time experience for e.g.: cyberspace, cyber terrorism, cybernetics, cyberpunk etc., same way there is a cyber society, where you can do what you do in real time environment i.e., you can meet, talk, share, discuss, business, interchange, your ideas/views to the unknown/known person sitting anywhere in the world. Not only this you can also get the desired information at your desk at a single click, also you can steal, hack, frighten, or spread terrorism, remotely without your physical presence. Cyber systems across the globe have many different rules governing the behavior of users. These users are completely free to join or leave any system whose rules they find comfortable or not comfortable to them. This flexibility may at times lead to improper user conduct. Also, in the absence of any suitable legal framework, it may be difficult to have a check on frauds, vandalism or abuses, which may cause the life of many online users miserable.

2. What's Different about Cyber Crime?

Cyber crimes—harmful acts committed from or against a computer or network—differ from most terrestrial crimes .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. 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 attacks4 may not be covered by outdated laws as protected forms of property.

2.1. Size of the Problem

Estimating the incidence, prevalence, cost, or some other measure of computer related crime is a difficult challenge, unlike bank robberies or fatal motor vehicle accidents, computer related crimes tend to defy quantification. Some of the most deftly perpetrated offences with or against information systems are never detected, not even by their victims; of those which are, some are concealed from authorities because disclosure could prove embarrassing or commercially inconvenient to victims. Victims may also believe, rightly or wrongly, that there is not much that police can do to assist them. Those offences which are detected can be difficult to cost. It may be instructive to look at cost on three dimensions There can be direct out of pocket losses sustained by the victim; costs in lost productivity while one's systems are "down"; costs involved in repairing and securing information systems which have been subject to attack; and the costs of economic opportunities foregone when individuals avoid e-commerce because of lack of trust.

2.2. Types of Cyber Crime

Cyber Crime comes in many forms and in many ways. Below mentioned are the different types of Cyber crime:

- **Communications in Furtherance of Criminal Conspiracies**

  Just as legitimate organizations use the information networks for record keeping and communication, so too are the activities of criminal organizations enhanced by the advent of information technology. There is evidence of information systems being used in drug trafficking, gambling, money laundering and weapons trade just to name a few.

- **Telecommunications Piracy**

  Digital technology permits perfect reproduction and easy dissemination of print, graphics, sound, and multimedia combinations. This has produced the temptation to reproduce copyrighted material either for personal use or for sale at a lower price.

- **Electronic Money Laundering**

  For some time now electronic funds transfers have assisted in concealing and moving the proceeds of crime. Emerging technologies make it easier to hide the origin and destination of funds transfer. Thus money laundering comes to the living room.

- **Electronic Vandalism and Terrorism**

  All societies in which computers play a major role in everyday life are vulnerable to attack from people motivated by either curiosity or vindictiveness. These people can cause inconvenience at best and have the potential to inflict massive harm.

- **Sales and Investment Fraud**

  As electronic commerce or e-commerce as it is called becomes more and more popular, the application of digital technology to fraudulent crime will become that much greater.

- **Illegal Interception of Information**

  Developments in telecommunications as well as data transfer over the net have resulted in greater speed and capacity but also greater vulnerability. It is now easier than ever before for unauthorized people to gain access to sensitive information.

- **Cyber Pornography**

  Spread of Child pornography and sexually implicit material.

- **E-murder**

  By manipulating medical prescription in a hospital.

- **Political Crime**

Abusive management of public funds by altering computer data. Bribery and corruption by manipulating data, manipulation in election by adding more votes or denial of voting rights.

- **Information Piracy and Forgery**

  Digital technology permits perfect reproduction of the original documents, examples are birth certificates, passport, false identity, counterfeiting of currency, negotiable instruments etc.
- **Hacking**

  Information theft from computers hard disk, removal storage etc. Data theft, data destroy, stealing and altering information.
- **Internet time thefts**

  By stealing user name and password, criminals use for themselves and steal the internet time allotted to the purchaser.
- **Hate/Communal Crimes**

  As building a web page is not expensive and reaches to billions of people, criminals spread hate or communal information or rumours, by building a website and also recruits people for their operation through advertisement.
- **Altering Websites**

  The hacker deletes some pages of a website, uploads new pages with the similar name and controls the messages conveyed by the web site.

3. Investigating the technical issues of Cyber crime

3.1. Defending against predefined cyber attacks

Agencies must identify all network access points and verify that the safeguards for the network and individual systems are adequate and operational. These systems include, but are not limited to: wireless access points, network access points, and network-attached devices. These controls include:

- Securing interfaces between agency-controlled and non-agency controlled or public networks.
- Standardizing authentication mechanisms in place for both users and equipment.
- Controlling users' access to information resources.

3.2. Defending against predefined internal attacks

- To defend against insider attacks on agency networks and to prevent internal damage, access rights to files shall be controlled to maximize file integrity and to enforce separation of duties.
- Access to files shall be granted only on as required for the performance of job duties.
- Networks that serve different agencies or departments shall be segregated, and access to those segmented networks shall be established as appropriate through the use of VLANs, routers, firewalls, etc.
- Access badges shall be programmed to allow entry only into assigned places of duty.
- Separation of duties in programming shall be enforced to eliminate trapdoors, software hooks, covert channels, and Trojan code.
- Users' activities on systems shall be monitored to ensure that users are performing only those tasks that are authorized and to provide an appropriate audit trail.

3.3. Defending against opportunistic Cyber crime attacks

To protect against opportunistic cyber crime attacks, authentication mechanisms shall be required before access is granted to any agency network resource. Authorization levels shall be reviewed regularly to prevent disclosure of information through unauthorized access. Vulnerability assessments and penetration tests are tools that can minimize opportunities for cyber crime and are part of a defense-in-depth strategy.

Each agency shall have the following responsibilities:

- To appropriately secure all hosts that could be a potential target for a denial of service (DoS) or distributed denial of service (DDoS) attack based on the agencies ability to accept the risk for a possible disruption in service from a successful attack.
- To deny all inbound traffic by default, thus limiting the channels of network attacks.
- To periodically scan for bots (software robots) and Trojan horse programs. Statewide Information Technology Standards
- To deploy authentication mechanisms wherever possible.
- To design and implement networks for maximum availability.
- To develop specific plans for responding to DoS and DDoS attacks in the agency incident management plan and the business continuity plan.

3.4. Defending against Hackers

To defend against hackers, it is critical to limit the amount of potential exploits within the network infrastructure. The following duties shall be performed by system administrators:

- Periodic scanning for spyware, adware and bots (software robots) with one or more anti-spyware programs that detect these malicious programs.
- Denial of all inbound traffic by default through the perimeter defense. Exceptions for traffic essential for daily business must be requested through network security.
- Provision of security awareness training to personnel on an annual basis that, in part, cautions against downloading software programs from the Internet without appropriate agency approval and outlines the process for addressing virus or other malicious threats to the network. This training should also stress the potential exposure that email attachments presents to the agency and employee.
- Deployment of intrusion detection and/or intrusion prevention systems, as appropriate.

3.5. Handling Virus warnings

To minimize the threat of hoax virus warnings, incident management procedures shall contain a provision that virus threats are verified before warnings about them are distributed. Appropriately verified warnings shall be distributed by management, agency security administrators, or the ITS Information Security Office through recognized government or verified vendor source, according to State and agency standards, policies and procedures. Virus detection programs and practices shall be implemented throughout agencies. Training must take place to ensure that all computer users know and understand safe computing practices. All agencies shall be responsible for ensuring that they have current software on their network to prevent the introduction or propagation of computer viruses. Agencies shall select and use virus prevention and mitigation standards and best practices as appropriate.

Virus controls, procedures, education and training shall include the following:

- Use of antivirus software.
- Performing frequent backups on data files.
- Use of write-protected program media, such as diskettes or CDROMs.
- Validating the source of software before installing it.
- Scanning for viruses on files that are downloaded from the Internet or any other outside source.
- Scanning for viruses on all diskettes, CDs or other media brought from home or any other outside source.
- Requirements that users first obtain management approval before directly adding any software to the system, whether from public software repositories, other systems or their home systems.

3.6. Installing Virus scanning software

Agencies shall install robust antivirus software on all LAN servers and workstations, including those used for remote access to the State network. In addition, system antivirus software, including virus signature files, shall be promptly updated as updates are released by the software vendor. System configuration management shall include:

- Maintenance of good backups of critical data and programs.
- Periodic review of overall controls to determine weaknesses.
- Prohibition of network connections to outside organizations without a mutual review of security practices.
- Configuration reports shall be maintained of all installed software, including the operating system. This information will be necessary if the software must be reinstalled later.

3.7. Collecting evidence for cyber crime prosecution

In the event of an active cyber crime, management has the authority to decide whether to continue collecting evidence or to lock down the system involved in the suspected crime. When dealing with a suspected cyber crime, agencies shall:

- Make an image of the system (including volatile memory, if possible) so that original evidence may be preserved.
- Make copies of all audit trail information such as system logs, network connections (including IP addresses, TCP/UDP ports, length, and number), super user history files, etc.
- Take steps to preserve and secure the trail of evidence.
- Report the incident to the ITS Information Security Office within twenty-four (24) hours, as required by law.

4. Conclusion

Cyber crime is everyone's problem. There is no doubt that the Internet offers criminals unparalleled opportunities. And its time we did something to protect ourselves. Information is the best form of protection. Concrete measures must be found in order to track electronics evidence, classify the material that needs to be search, and their preservation, so that systems are better protected from cyber intrusions. In addition, new rules and regulations must be developed by law enforcement agencies to address the various families of computer crime. Appropriate practical measures and policies should be taken with more human and financial resources should be devoted, Joint research and co-operation agreements should be promoted both in countries and between countries including guidance concerning best practices so that a very common man should know the dark side of this world before entering into it and should not become a victim but, take the maximum benefits out of it.

5. References:

[1] Bangkok International Summit (2007) Declaration on Policing Cyberspace K. Jaishankar[1] Manonmaniam Sundaranar University, Tirunelveli, India Bessie Pang[2] .The Society for the Policing of Cyberspace (POLCYB), Canada .Stuart Hyde[3] Assistant Chief Constable, West Midlands Police, United Kingdom

[2] David Wrighta, Serge Gutwirthb, Michael Friedewaldc, Paul De Hertb, Marc Langheinrichd and Anna Moscibrodab, Privacy, trust and policy-making: Challenges and responses Computer Law & Security Report, Volume 25, Issue 1, 2009, Pages 69-83.

[3] Rolf H. Webera, Transparency and the governance of the Internet, Computer Law & Security Report, Volume 24, Issue 4, 2008, Pages 342-348.

[4] Ramifications of Cyber Crime and Suggestive Preventive Measures.Jivesh Govil, SJtiuvdeesnht GMoevmilb, eSrt,u IdEeEntE M ember, IEEE and Jivika Govil Dept. of Electrical Engineering & Computer Science University of Michigan, Ann Arbor, Michigan, USA jivesh@umich.edu Jivika Govil Dept. of Information Tech. and Computer Science Apeejay College of Engineering, MD University Gurgaon, Haryana, India jivikag@email.com

[5] A Guide To Cyber-Crime Investigations ,August Bequai,Legal Editor,7921~otws Branch Drive, Suite 133, Mcban, VA 22102, 1JSA.

[6] Computing Crime: Information Technology, Police Effectiveness, and the Organization of Policing _ Luis Garicano University of Chicago and CEPR Paul Heaton University of Chicago December 4, 2006

[7] Internet crime Cyber Crime – A new breed of criminal? Kit Burden & Creole Palmer, Barlow Lyde & Gilbert

[8] Marcus Turlea, Data security: Past, present and future Computer Law & Security Report, Volume 25, Issue 1, 2009, Pages 51-58.