Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (58-61), Month: January-April 2016, Available at: www.noveltyjournals.com

# Cybersecurity: Model for Cybercrime Prevention and Controlling

Dr. P.B. Pathak

Assistant Professor & Head, Department of Computer Science & Information Technology Yeshwant Mahavidyalaya Nanded Maharashtra, India

***Abstract:*** **Computer may be the target of the offense; attacks on network confidentiality, integrity and / or availability i.e. unauthorized access to and illicit tampering with systems, programs or data or computers may be in supplementary role in the commission of a traditional offense. Cybercrimes range from economic offenses fraud, theft, espionage, sabotage and extortion, product piracy, etc. to infringements on privacy, propagation of illegal and harmful content, facilitation of prostitution and other moral offenses, and organized crime. At its most severe, Cybercrime borders on terrorism, encompassing attacks against human life and against national security establishments, critical infrastructure, and other vital veins of society.**

***Keywords:*** **Cybercrime; Cybercriminal; Cybersecurity; Cyberlaw; Threat; Vulnerability; Prevention; Controlling; Multilayer.**

## 1. INTRODUCTION

In The scope of study of Cybercrime is very broad since there exists n number of possibilities of commission Cybercrime. There exits various definitions of the term Cybercrime, all are attempting to explain scope of Cybercrime. These multiple possibilities come from different hardware and software vulnerabilities. The paper contains detailed study of the network and internet hardware and software's and the points of possible vulnerabilities, various definitions of security and meaning and types of security incidents. The list security threats and vulnerability is very long, attempt is made to study maximum but they are endless. The main subject matter of the paper is the series of safeguards against attacks, incidents and thereby commission of Cybercrime by Cybercriminals. The paper attempts to answer questions what are the Cybercrime prevention and controlling steps i.e. safeguards based on the discussion of all the components, technology, hardware software used in computer network, communication and information system. Attempt is also made for the in depth study and discussion of safeguards in case of software and hardware. The paper gives a Model for Cybercrime Prevention and Controlling steps. I hope that this Model for Cybercrime Prevention and Controlling Measures will serve as a foundation to understand and effectively take action in Prevention, Detection.[2,14]

## 2. MODEL FOR CYBERCRIME PREVENTION AND CONTROLLING

Model for Cybercrime Prevention and Controlling Measures primarily consists of Law aspect, technological aspect. Fighting Cybercrime is technical, juridical and ethical issue. Technological aspect is considered here for development of the paper. Criminals in general and Cybercriminals do not bother about ethics. A strategy to tackle the emerging problem of Cybercrime should have the essential components as Uniform Cyberlaws all over the Globe, Multilayer Security Solutions comprising of Physical Security, Hardware Security, Software Security, Interpol like Internetpol Agency and Miscellaneous Measures[1,7]

***Uniform Cyberlaws all over the Globe:***

The nations have their own set of Cyberlaws. Most of the countries even don't have separate Cyberlaws in place. To deter the Cybercriminals every nation having Computer infrastructure should have Cyberlaws. There should be Forensics readiness not only to prevent but when Cyber Incident takes place, for the purpose of gathering evidences to prosecute Cybercriminals. Attempt should be made to make the uniform Cyberlaws. There is dire need of Cybercrime Convention,

truly an international treaty designed to police Cybercrime through international cooperation. Cybercrime Prevention and Controlling Measures requires a approach. Collaboration between government, industry, private sector, and users is crucial when developing strategies to deal with Cybersecurity threats that undermine confidence and trust in the online environment, Countries all over the globe are to be encouraged to take every opportunity for to come together to share experiences, and work towards their common objectives in promoting a culture of cybersecurity that will foster an inclusive, secure and global information society.[3,15]

***Multilayer Security Solutions:***

The model is essentially stressed on enforcing Multilayer Security consisting of Physical Security, Hardware Security and Software Security. Providing Security is safeguarding the Integrity, Confidentiality, Availability, Reliability and Security of Computer Systems and Networks. Multilayer Security ensures Computer Security and Network Security by applying Strong Authentication Techniques, by keeping Forensic Readiness. Factors affecting Security are Misconfigurations of Computer Systems, Poor User and Administrator Education, Poor Software Design, Network and System Design Issues, Substandard Operational Procedures, Use of Insecure Protocols, Weak Passwords, and finally, Lack of Awareness & Indifference.[4,6]

***Physical Security:***

Physical Security can be provided by Physical Access Control. Ensuring physical access control generally includes Securing the Servers, Securing the Workstations, Securing the Network Devices, Securing the Cables, Security Considerations for Wireless Networks, Security Considerations for Portable Computers, Printed Data Security, Removable Storage Security.

Cryptography is having very important role in Physical Access Control. The cryptography is the science of transforming clear, meaningful information into an enciphered, unintelligible form using an algorithm and a key. Cryptographic techniques include: Encryption and Steganography. Encryption involves applying a procedure called an algorithm to plain text to turn it into something that will appear to be gibberish to anyone who doesn't have the key to decrypt it. Steganography is a means of hiding the existence of the data, not just its contents. This is usually done by concealing it within other, innocuous data.[5,8]

***Hardware Security:***

Hardware Security comes in the form of Security of Network devices which are generally dedicated computers themselves, running proprietary software's like Firewalls, Routers and Switches. Other hardware based components of Network security may include devices that provide extra security for authentication, such as: Smart Card Readers, Biometric authentication devices- Fingerprint Scanners, Retinal scanners and Iris scanners, Voice Analysis Devices. These devices provide a high level of security environments for secure and reliable network authentication. [11, 13]

***Software Security:***

Software Security covers broader range than do hardware Security. These solutions include the security features built into the network operating system as well as additional security software made by the operating system vendors or third party vendors. Digital Signature, XML aware digital signature, Digital Certificates, Auditing, Redundancy, Software Based Firewalls, Public Key Infrastructure, Integrated Intrusion Detection Systems are some Software Security measures.

***Interpol like Internetpol Agency:***

There is an urgent need of some Interpol like Internetpol agency which will have authority to grab the global criminals by International Cooperation considering the global nature of Cybercrime.[6,10]

***Important diverse dealings:***

- Cybersecurity: Security Monitoring, Audit, Advanced Analytics, Agile and Collaborative Response, Innovative Security Controls are very important legs of Cybersecurity.
- In built Security Features: Emphasis should be on adequate in built security features in the computer system, Devices, and Computer Networks.

- Security Culture: An approach that emphasizes an information security culture within the organization.
- Writing a Secured Code: The code written for Computer, Computer Network devices and other devices for Computer infrastructure should be fully secure.
- Full proof CIIP: Critical Information Infrastructure Protection Mechanism should be full proof to eliminate danger of Cyberterrorism.
- Firewall Protection: Firewalls protect a user from unauthorized access attacks while on a network. They provide access to only known and authentic users. Also consider Penetration Testing.
- Frequent Password Changing: With the advent of multi user systems, security has become dependent on passwords. Thus one should always keep passwords to sensitive data secure. Changing them frequently and keeping them sufficiently complex in the first place can do this. Make the password strong.
- Safe Surfing: Safe surfing should be followed by all users on a network. Safe surfing involves keeping ones e-mail address private, not chatting on open systems, which do not have adequate protection methods, visiting secure sites. Accepting data from only known users, downloading carefully, and then from known sites also minimizes risk.
- Frequent Virus Checks: One should frequently check ones computer for viruses and worms. Any external media should always be virus checked before running.
- Email Filters: Email filters monitor the inflow of mails to the inbox and delete automatically any suspicious or useless mails thus reducing the chances of being bombed or spoofed.
- Backup Confidential Data: Backing up your data is the simplest way to keep you safe from disaster. The backup process will allow you to recover your data if any catastrophic event occurs. While it may seem repetitive and cumbersome, it is cheap and reasonably simple and could save you from bankruptcy.
- Reducing Opportunity: Cybercrime or likely threats or actions require the development and deployment of a new Internet architecture more resilient to wrongful use for destructive purposes, more powerful encryption, significantly more powerful intrusion prevention systems, more securely developed operating and applications software, better and more timely patch capabilities, and intelligent digital agents residing on the networks of the world that can sense and mitigate digital threats.

Attack Prevention: Configure Systems Conservatively, Install Updates Instantly, Encrypt Communication, Control Configuration of Routers, Separate Services, Establish Assessments and Certificates, and Prepare Emergency Plans.[9,12]

## 3. CONCLUSION

Cybercrime is already a big problem all over the world and it's growing fast. Cybercrime is a social problem as well as a legal one. Application of tactics and techniques, including the legal system, peer pressure, and existing and emerging technologies, needed to prevent Cybercrime. Unless appropriate steps are taken to protect ourselves against Cyberattacks whole world will surely suffer tragic Cyberattacks that will have devastating impacts on our economy and will include loss of life. The only way to stop Cybercrime is joint operation and sharing knowledge and expertise in different areas to fight Cybercrime. There must be a coherent approach taken by lawmakers, companies and consumers alike if Cybercrime is ever going to become a manageable problem. Cybercrime is on the increase and is not going to go away. Unless steps are taken to improve awareness of the types of attacks that a typical Internet user could be subject to, the situation is not going to improve.

Ever expanding area of Computer and Computer Networks both wired and wireless, generating new threats and vulnerabilities continuously thereby generating new techniques and opportunities for commission of Cybercrime so as the new preventive measures. Every threat, vulnerability and new technique for commission of Cybercrime can be a separate topic of research.

## REFERENCES

[1] Bluefire Security Technologies. (2003) "Mobile insecurity: A practical guide to threats and vulnerabilities." http://www.bluefiresecurity.com

[2] Clyman J. (2004). "Understanding Directory Harvest Attacks; ever wonder how spammers got your carefully guarded e-mail address?" PC Magazine.

[3] Shaffter G. "Good and Bad Passwords How-To: Password Cracking Goals, Techniques and Relative Merits and Cracking Times of Different Techniques."

[4] http://geodsoft.com

[5] Australian Computer Emergency Response Team, (2004), "Computer Crime and Security Survey", Queensland University, Brisbane, Australia.

[6] Daon (2003) "Biometrics and PKI based Digital Signatures." A Short White Paper http://www.daon.com

[7] Champion M., Ferris C, Newcomer E, & Orchard D. (2002). "Web Services Architecture." http://www.w3.org

[8] Lange L. (2003) "Web Services Security Gets Serious." http://www.techweb.com

[9] Verdelho P (2008) "The effectiveness of international co-operation against cybercrime: examples of good practice." For the Project on Cybercrime of the Council of Europe, 2008.

[10] Anat H & John D. A. (2003) "The impact of denial-of-service attack announcements on the market value of firms." Risk Management and Insurance Review.

[11] Baker W. H. & Wallace L. (2007) "Is information security under control?" IEEE Security & Privacy.

[12] Foltz C. B. (2004) "Cyberterrorism, computer crime, and reality." Information Management & Computer Security

[13] Microsoft. (2007) "Security Guidance Center." http://www.microsoft.com

[14] Yan Zhang, Jun Zheng, and Miao Ma.(2008)" Handbook of Research on Wireless Security." Idea Group Inc (IGI)

[15] Chapell, Laura. "Cyber Crime – It Could Happen to You." Computer Crime Research Center

[16] Davis, Mark (2005). "Network Security and Encryption." Dublin Institute of Technology: http://www.electronics.dit.ie.