Shabd Braham
E ISSN 2320 – 0871
International Research Journal of Indian languages
17 December 2017
Peer Reviewed Refereed Research Journal

Internet Hacking and Prevention Strategies

Palak Khandelwal
Assistant Professor
Chameli Devi group of Professional Studies
Indore, M.P., India

Abstract

Internet hacking is evolving at an astounding pace, following the same dynamic as the inevitable penetration of computer technology and communication into all walks of life. There are a huge number of cyber threats and their behavior is difficult to early understanding hence difficult to restrict in the early phases of the cyber attacks. Cyber attacks may have some motivation behind it or may be processed unknowingly. The attacks those are processed knowingly can be considered as the cyber crime and they have serious impacts over the society in the form of economical disrupt, psychological disorder, threat to National defense etc. cyber crime is not a matter of concern for India only but it is a global problem and therefore the world at large has to come forward to curb this menace. The internet in India is growing rapidly. It has given rise to new opportunity in every field like – entertainment, business, sports, education etc. It is universally true that every coin has 2 sides, same for the internet, it uses has both advantage and disadvantage, and one of the most disadvantage is Cyber-crime. We can say, cyber-crime is any illegal activity which is committed using a computer network (especially the internet). Also, cyber-crime involves the breakdown of privacy, or damage to the computer system properties such as files, website pages or software.

Key Words: *Cyber Crime, Cyber attacks, Internet*

Introduction

'Cyber crime' combines the term 'crime' with the root 'cyber' from the word 'cybernetic', from the Greek, "kubernân", which means to lead or govern. The "cyber" environment includes all forms of digital activities, regardless of whether they are conducted through networks and without borders. The term cyber crime can be defined as an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction. . The Internet space or cyber space is growing very fast and as the cyber crimes. Some of the kinds of Cyber-criminals are mentioned as below.

- Crackers: These individuals are intent on causing loss to satisfy some antisocial motives or just for fun. Many computer virus creators and distributors fall into this category.
- Hackers: These individuals explore others' computer systems for education, out of curiosity,
  or to compete with their peers. They may be attempting to gain the use of a more powerful computer, gain respect from fellow hackers, build a reputation, or gain acceptance as an expert without formal education.
- Pranksters: These individuals perpetrate tricks on others. They generally do not intend any particular or long-lasting harm.
- Career criminals: These individuals earn part or all of their income from crime, although they Malcontents, addicts, and irrational and incompetent people: "These individuals extend from the mentally ill do not necessarily engage in crime as a full-time occupation. Some have a job, earn a little and steal a little, then move on to another job to repeat the process. In some cases they conspire with others or work within organized gangs such as the Mafia. The greatest organized crime threat comes from groups in Russia, Italy, and Asia. "The FBI reported in 1995 that there were more than 30 Russian gangs operating in the United States. According to the FBI, many of these unsavory alliances use advanced information

Shabd Braham
E ISSN 2320 – 0871
International Research Journal of Indian languages
17 December 2017
Peer Reviewed Refereed Research Journal

technology and encrypted communications to elude capture ”(1).

- Cyber terrorists: There are many forms of cyber terrorism. Sometimes it's a rather smart hacker breaking into a government website, other times it's just a group of like-minded Internet users who crash a website by flooding.

The digital medium provides the convenient shield of anonymity and fake identities. Errant persons become more emboldened in their offensive behavior if they think that they will not face any consequences. In recent years, there have been numerous reports of internet users receiving unsolicited e-mails which often contains obscene language and amounts to harassment. Those who post personal information about themselves on job and marriage to websites or social networking websites are often at the receiving end of ‘cyber-stalking’. Women and minors who post their contact details become especially vulnerable since lumpen elements such as sex-offenders can use this information to target potential victims

II. Aspect of Cyber-Crime

Technological Aspect of Cybercrime

From a technological dimension, other experts point out the need for a comprehensive term, such as *"electronic crime"* or *‘e-crime’*, thanks to the convergence of ICT, including mobile technology, telephony, memory. These electronic media will be targeted increasingly more often and will also be used to conceal, commit, or support crimes and offenses.

Anthropological Aspect of Cybercrime

From an anthropological aspect, cybercrime originates from various populations and exhibits socio-educational, socio-economic, and techno-ideological factors and their expressions, including pathological expressions like addiction. Difficult socio-economic conditions also include the Internet as a place for expressing psychological troubles with socio-economic origins, including theft, child pornography, and calls for uprisings, violence, and hatred.

Strategic Aspect of Cybercrime

From a strategic aspect, cybercrime is seen as an offense to cyber-security, namely attacks to digital networks for the purpose of seizing control, paralysing them, or even destroying infrastructures that are vital to governments and sectors of vital importance.

Iii. Impact Of Cyber Crime/Internet Hacking

1. Potential Economic Impact

Productivity is also at risk. Attacks from worms, viruses, etc take productive time away from the user. Machines could perform more slowly; servers might be in accessible, networks might be jammed, and so on. Such instances of attacks affect the overall productivity of the user and the organization. It has customer service impacts as well, where the external customer sees it as a negative aspect of the organization. In addition, user concern over potential fraud prevents a substantial cross-section of online shoppers from transacting business. It is clear that a considerable portion of e-commerce revenue is lost due to shopper hesitation, doubt, and worry. These types of consumer trust issues could have serious repercussions and bear going into more detail.

2. Impact on Market Value

The economic impact of security breaches is of interest to companies trying to decide where to place their information security budget as well as for insurance companies‘ that provide cyber-risk policies. This new and evolving view of damage becomes even more important as many firms rely on information systems in general and the Internet in particular to conduct their business. This precedent may force many insurance companies to compensate businesses for damage caused by hacker attacks and other security breaches. A market value approach captures the capital market‘s expectations of losses resulting from the security breach. This approach is justifiable because often companies are impacted more by the public relations exposure than by the attack itself .Moreover,

Shabd Braham
E ISSN 2320 – 0871
International Research Journal of Indian languages
17 December 2017
Peer Reviewed Refereed Research Journal

managers aim to maximize a firm‘s market value by investing in projects that either increase shareholder value or minimize the risk of loss of shareholder value. Therefore, in this study we elected to use market value as a measure of the economic impact of security breach announcements on companies

Impact on Consumer trust

Since cyber-attackers intrude into others‘ space and try and break the logic of the page, the end customer visiting the concerned page will be frustrated and discouraged to use the said site on a long term basis. The site in question is termed as the fraudulent, while the criminal masterminding the hidden attack is not recognized as the root cause. This makes the customer lose confidence in the said site and in the internet and its strengths.

Impact on Perception

The impact of cybercrime is hard to identify. Yet, there is an increase in the development of information technology and the exploitation of vulnerabilities among cybercriminals, a gap between lawful and corrupt countries, and a paradox related to technological developments and breakthroughs. It is always worthwhile to remember that technology itself is neutral. However, its use can be described as negative or positive.

The Types of Cyber Crime

As per my research all cyber crimes may broadly be categorized in –

- Crimes based on personal issues
- Crimes Related to Telecommunication

Crimes related to Telecommunication

Communication crimes of this category basically affect the large group of peoples. When an organization is mostly depends on Digital Information System and using that for the activities which are illegal in aspects of law come under the Telecommunication Cyber Crime. Cyber Criminals are using different front end services to hide their actual profession. People use others telecommunication services illegally and without the knowledge of the owner. The third category of telecommunication crime is piracy of digital content. When we publish any ones personal objectionable data without bringing that in their knowledge comes in this category of telecommunication theft

Crimes based on personal issues

People unknowingly just for fun may send an email or make unauthorized access to another user 's space. They may do not have any intention to commit crime but for fun or for fake repo may indulge in with such activities. A Person may Steal the identity of his higher authority and can steal the confidential data for black money. A psychologically sick person may disseminate malicious software or viruses to harm other people being sick from progress of his/her colleagues.

Cyber Crimes against Individuals

1. Email bombing

This is a serious crime in which a person sends a number of emails to the inbox of the target system. Mail bombs will usually fill the allotted space on an email server for the user e-mail and can result in crashing the e-mail server.

2. Hacking

Among the all types of cybercrime it is the most dangerous and serous thread to the internet and e-commerce .Hacking simply refers to the breaking into the computer system and steals valuable information from the system without any permission. Hacking is done by hackers now the question arises who are hackers, hackers are in between client and server and able to spoof the data /info. Duplication the IP address illegally.

3 .Spreading computer virus

It is a set of instruction which is able to perform some malicious operations. Viruses stop the normal function of the system programs and also to the whole computer system. They can also ruin/mess up your system and render it unusable without

Shabd Braham
E ISSN 2320 – 0871
International Research Journal of Indian languages
17 December 2017
Peer Reviewed Refereed Research Journal

reinstallation of the operating system A computer viruses can be spread through—Emails ,Cds, Pen drives (secondary storage),Multimedia, Internet.

4. Phishing

Phishing simply refers to steal information like passwords, credit card details, usernames etc. over the internet. Phishing is typically carried out by email spoofing and instant messaging. In this type of crime hackers make a direct link which directs to the fake page /website which looks and feel like identical to the legitimate one.

5. Identity theft

It simply refers to fraud or cheat others by make their wrong identity of others

6. Malicious Software

These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

7. Cyber warfare

It is Internet-based conflict involving politically motivated attacks on information systems. Cyber warfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems -- among many other possibilities

8. Domain hijacking

It is the act of changing the registration of a domain name without the permission of its original registrant.

9. SMS Spoofing

SMS Spoofing allows changing the name or number text messages appear to come from.

Prevention Strategies

More recent versions of Cybercrime is considered one the most dangerous threats for the development of any state; it has a serious impact on every aspect of the growth of a country. Government entities, non-profit organizations, private companies and citizens are all potential targets of the cyber criminal syndicate. Cyber criminals are no different than traditional criminals in that they want to make their money as quickly and easily as possible. Cybercrime prevention can be achieved fairly quickly and in a cost-effective manner. The prevention of cyber criminal activities is the most critical aspect in the fight against cybercrime. It's mainly based on the concepts of awareness and information sharing. A proper security posture is the best defense against cybercrime. Every single user of technology must be aware of the risks of exposure to cyber threats, and should be educated about the best practices to adopt in order to reduce their 'attack surface' and mitigate the risks.

Conclusion

The risks of cyber crime are very real and too ominous to be ignored. Every franchisor and licensor, indeed every business owner, has to face up to their vulnerability and do something about it. At the very least, every company must conduct a professional analysis of their cyber security and cyber risk; engage in a prophylactic plan to minimize the liability; insure against losses to the greatest extent possible; and implement and promote a well-thought out cyber policy, including crisis management in the event of a worst case scenario.

References

1 Bowen, Mace (2009), Computer Crime, Available at: http://www.guru.net