Cybercrime

Name

Institution

Cybercrime

Cybercrime involves the use of computers and networks to commit crimes. With the advancement in technology, computers can be used to commit crimes or to target victims. Criminals commit these offenses against groups or individuals with the motive of harming the victims' reputation intentionally, cause mental or physical harm either directly or indirectly. These criminal activities are aided by the use of modern telecommunication technology such as mobile phones and the internet. This type of crime can adversely affect the financial security of both the government and the private sector. Organizations, government and the citizens should enact appropriate security measures to mitigate the possibilities of becoming victims of cybercrime.

Cybercriminals have advanced their illegal activities, making it possible for them to be involved in various criminal activities such as hacking, child pornography, and copyright infringement. These illegal activities have no borders and can either be virtual or physical. Cybercrime can be divided into three broad categories, which include abuse such as sexploitation, financial crimes like online corruption and phishing, and computer software and hardware attacks like network intrusion and malware. Cybercrime can be classified into different groups depending on their targets and effects on victims.

Computer communications systems in an organization or between individuals can be denied service because of the criminal activities of malicious hackers. This type of criminal attack is referred to as Cyber extortion. The hackers can regularly disrupt computer-based communications such as the use of emails or hack organizational websites and later demand money to stop their attacks. Cybercriminals target corporations and organizations that have a

strong financial base, cripple their networking operations and demand for cash to restore the service. The denial of service strategy can make an organization lose its reputation due to the inability of its customers to access the website leading to loss of revenues.

Another cybercrime activity is cyberterrorism. Cyber-terrorists coerce or intimidate organizations, individuals or the government by launching an attack on their computer networks and any information stored on their computers. This is the act of terrorism that is committed to the use of computer resources or cyberspace (Moore, 2014). The cybercriminals can spread propaganda that there will be insecurity in some regions or town without specifying a particular date. Information on insecurity is a concern to any government and the citizens. The propaganda forces the authorities to increase their security detail to combat any incidence of insecurity. Cybercriminals can also participate in hacking activities that are directed towards families, individuals or organizational networks. Their primary intention includes creating fear or collecting useful information that can be used to blackmail or rob organizations and individuals.

When computers are used to target individuals, they become a tool for cybercrime instead of being a target. This type of cybercrime does not involve the use of technology because the terrorists target the weaknesses of the individual. They cause psychological damage to their victims, and this makes it difficult for the individual to take legal action. The government, organizations and the citizens must put appropriate measures in place to ensure that they eliminate all cybercrime activities. Cybercrime adversely affects the way business activities are carried out and can lead to the closure of reputable organizations. Everyorganization should enforce internationally accepted cybersecurity measures with the attempt of curbing cybercrime. If these strategies are implemented, the cybercriminals will find it difficult to perform their illegal activities.

References

Moore,R. (2014). *Cybercrime: Investigating high-technology computer crime*. Newark, NJ: LexisNexis/Matthew Bender.