A Study on Implementation of Cyber Security to Reduce the Cybercrimes

Shambhu Bhardwaj, Associate Professor
College Of Computing Sciences And Information Technolog, Teerthanker Mahaveer University,
Moradabad, Uttar Pradesh, India
Email id- shambhu.bharadwaj@gmail.com

ABSTRACT:** **Any illegal behavior involving a computer, a device on the network, or a network is considered a cybercrime. Whereas most cybercrimes are committed to making money for the perpetrators, certain cybercrimes are committed against computers and other devices immediately to harm or destroy them. The susceptibility of e-businesses to cybercrime is a serious issue. Cybercrime refers to any illegal conduct carried out online, including spoofing, phishing, botnet, or denial-of-service assaults that result in financial losses for e-commerce businesses. This paper gives instances of several businesses that have been impacted by typical cybercrimes and illustrates how they are committed. Additionally, some advice on crime prevention is provided. Internal auditors would benefit from knowing the different forms of cybercrime as well as the fundamental preventive methods since they may assess if a business has effective cybercrime defenses. In this paper, the author talks about cybercrimes, types of cybercrimes, and preventive measures. In the future, this paper will aware of cybercrimes or preventive steps.

KEYWORDS:** **Cybercriminals, Cybercrime, Computer, Internet, Software.

1. INTRODUCTION

Cybercriminals steal consumers' personal computers, mobile data, and personal information from social media, commercial secrets, and other information using the internet or computer technology. Criminals who engage in these unlawful online operations are known as hackers. Even while law enforcement organizations are working to address this issue, it keeps becoming worse and more people are falling prey to identity fraud, hacking, and dangerous software. Using opaque security that employs a single system of hardware or software to verify any information that's also accessed via the Internet is among the greatest methods to block these crooks and secure critical information. Let's learn more about online crimes [1], [2].

1.1. Reasons for cybercrime:

Cybercriminals always choose the fastest route to large profits. They aim to steal sensitive data from wealthy individuals or wealthy institutions like casinos, banks, or financial enterprises where a lot of money is transacted regularly. It's challenging to apprehend these offenders. Consequently, this leads to a rise in cybercrimes worldwide. Laws are necessary to secure computers against hackers since they are vulnerable to them. We might cite the following causes for computers' vulnerability [3], [4]:

It is difficult to protect a computer system against unauthorized access since there are numerous ways for a breach to occur because the technology is so advanced. Access codes, retinal pictures, sophisticated audio recorders, etc. that could easily trick biometric technology or get past firewall could be stolen by hackers and used to get past numerous security measures. Ability to store information in a relatively small amount of space: The laptop has the special ability to store data in a very little amount of space. This makes it much simpler for individuals to steal data from other storage systems and utilize it for their financial gain [5], [6].

- *Complexity:* The operating systems that power a computer are made up of millions of lines of code. Because the human psyche is flawed, mistakes can be made at any time. Cybercriminals benefit from these openings.

- *Negligence:* one of the signs of human behavior is carelessness. So, now there is a chance that by failing to protect the computer system, they can give control and authority over the computer system to cyber criminals.

- *Loss of Evidence:* Crime-related information is quickly erasable. Hence the lack of evidence has become a very pervasive and obvious issue that incapacitates the system used to conduct cybercrime investigations.

1.2. Cybercrime categories:

The most prevalent cybercrimes are described below, while there are many others, which are shown in Figure 1.

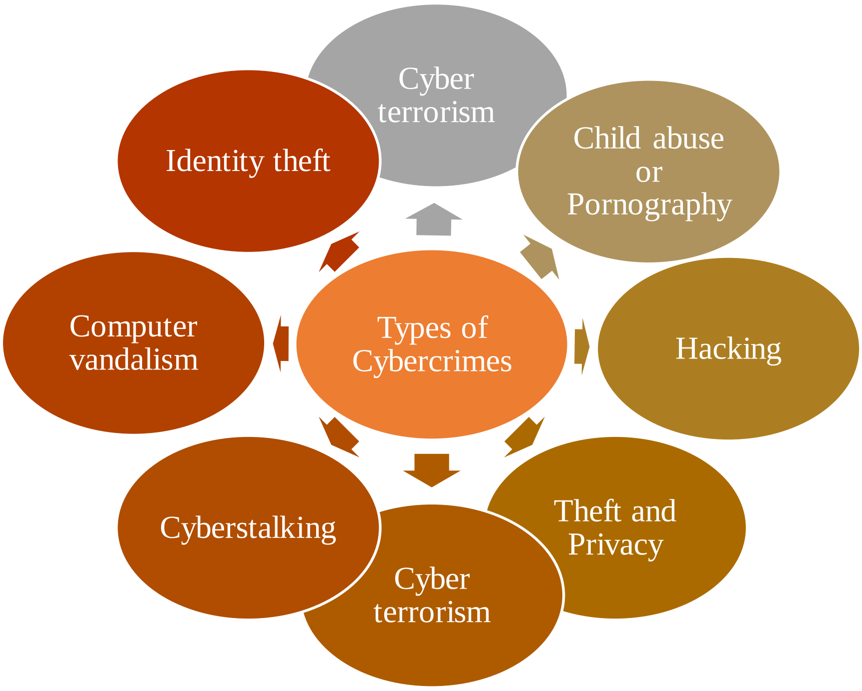

Figure 1: Illustrate the Types of Cybercrimes.

1.2.1. Child abuse or pornography:

Around the world, children are sexually abused over the internet in large numbers. This is another sort of cybercrime, where criminals use chat rooms to recruit children for the production of child porn. Every country's cybersecurity division spends a lot of time watching chat rooms that are popular with kids to curtail and stop child abuse and solicitation [7].

1.2.2. Theft and Privacy:

Downloading software, music, movies, and other media in violation of copyright laws is known as piracy or piracy. Yet peer-sharing websites that promote software piracy do exist, and the FBI is currently targeting many of these sites. The judicial framework is now dealing with this cybercrime, along with rules that prevent unauthorized downloading. Film directors or producers are often the targets of this crime.

1.2.3. Hacking:

Hacking is the straightforward phrase for transmitting unauthorized commands to some other computer system or network. In this instance, a person's computer has been compromised, allowing access to personal or sensitive data. The offender might not have been aware whether his computer has been accessed remotely since he utilizes a variety of applications to break into the victim's PC. Government sites are frequently a top target for hackers since doing so helps them become more well-known, which is then fueled by aggressive media attention. This differs from ethical hacking, which is a technique employed by several firms to assess the effectiveness of their Internet security measures [8], [9].

1.2.4. Cyber Terrorism:

Cyber terrorism is described as the act of Internet network that involves planned, extensive attacks as well as disruptions of networked computers using infected computers, or actual physical threats utilizing malware, to target people, governments, but also organizations. Cybercrime is also referred to as information warfare. The purpose of terrorism is to instill a sense of dread in the victims' thoughts. By keeping this idea in mind, it is simpler to distinguish between cyber-attacks and acts of cyber terrorism that are motivated by financial or narcissistic gain. The main focus of a cyber-terrorist's operations is to cause harm and devastation.

1.2.5. Cyberstalking:

Cyberstalking is a form of internet harassment in which the victim receives a constant stream of messages or emails. These stalkers generally know their targets, so instead of engaging in actual stalking, they turn to the Internet. To make the victims' life worse, they start offline stalking in addition to cyberstalking if they observe that it is not having the intended impact.

1.2.6. Identity theft:

Identity theft has grown to be a significant issue as more individuals use the Internet for financial transactions or banking services. In this type of cybercrime, a perpetrator gains access to a victim's checking account, debit card, credit card, Social Security number, and other personal information to steal money or make purchases online in the victim's name. It may cause the victim to suffer significant financial losses or possibly damage their credit history.

1.2.7. Computer Vandalism:

Computer vandalism is a form of hostile action that includes disrupting businesses by harming computers including data in various ways. The construction of malicious software intended to carry out damaging actions like deleting hard drive information or stealing login credentials is a common method of computer vandalism.

2. DISCUSSION

2.1. How can cybercrime be combated?

Establish multifaceted public-private partnerships with law enforcement organizations, the data technology sector, data security groups, internet corporations, including financial institutions to combat cybercrime. Cybercriminals do not compete with one another for dominance or control like they do in the physical world. Instead, they cooperate to develop their abilities and even support one another in finding new possibilities. Therefore, the traditional means of criminal justice cannot be applied to cyber criminals.

Utilizing the solutions offered by Cross-Domain Solutions is the best course of action. This enables companies to employ a single system made up of both software and hardware to authenticate information access and transfer when it occurs between multiple security analysis methods. This enables smooth sharing of information or access inside certain tools and mechanisms but prevents the information from being intercepted or accidentally released to users outside of that security classification. This promotes the security of the network as well as the systems connected to it.

2.1.1. Protect your Mobile Devices:

Many individuals are unaware that unwanted software, including computer viruses or hackers, may also infect their mobile devices. Make cautious you only get software from reliable sources. Maintaining an updated operating system is also essential. Make careful to set up antivirus protection as well as a lockable storage screen. However, if you misplace your phone or merely leave it on the table for a little while, anybody may access all of your sensitive information. Even worse, someone may put malicious software on your computer and use your GPS to follow your every step.

2.1.2. Safeguard your data:

With your most sensitive information, such as bank records or tax returns, use encryption to safeguard your data. By learning about fraud and hacking techniques online, one may keep one step ahead of the hacker. Fishing is a well-known hacking technique, however by gathering knowledge on the most recent fishing assaults on the Internet, one may avoid any scams. Therefore, be cautious and warn your neighbors about these frauds [10]–[12].

2.1.3. Online Identity Protection:

It is preferable to be overly careful than underlying cautious when it comes to online identity protection. You must use extreme caution while disclosing personal information online, including your name, phone number, address, or financial information. When making online purchases or other transactions, ensure sure the websites are safe. To do this, you must enable your privacy controls when using or logging onto social media platforms.

2.1.4. Use Security Software to Safeguard your PC:

For basic internet security, several different types of security software are needed. With these, you can safeguard your device. Security software must include firewalls or antivirus software. A firewall is often the first line of defense for your computer. It controls what is permitted and who is permitted to communicate with your computer online. A firewall is like a "policeman" who monitors all data trying to enter and depart your computer over the Internet. It allows communications that it knows are secure while blocking "bad" traffic like attacks from ever reaching your system [13], [14].

2.1.5. Parental Control:

In the age of modern technology, people should keep track of their children's online activity. Giving children ample privacy would be difficult. Parents must exercise caution and monitor their children's browser history as well as email accounts frequently. A better method to handle this is to enable parental controls in mobile applications, browsers, and even at the router level so that kids can only visit secure sites. This should keep the youngsters safe from internet scams. Many programs, such as Netflix, YouTube, and Amazon Prime, provide tailored material for children to safeguard them from harm.

Rapid technology advancements have opened up a wide range of new opportunities and effective sources for businesses of all kinds. The internet has been a key driver of technological advancement. The internet has made the globe smaller by bringing far-off items closer together. The internet has evolved into a valuable national resource, and overall national security increasingly depends on it. However, these novel risks, such as cybercrime, also came along with the new technology. Cybercrime is any crime that involves the use of a computer, such as phishing, spamming, or hacking.

3. CONCLUSION

Today, there are a lot of hackers to be found all around the world. The FBI, CIA, and state police are just a few of the governmental and commercial agencies working to find these hackers, but we also must protect ourselves and our data from online theft. In addition, it is important to teach illiterate people how to use computers, the internet, debit cards, and credit cards. The easiest method to prevent these things is to be cautious and watchful, but all IDs including passwords on the Internet must be unique and strong. Since these hackers sit in one nation and target machines in another, we understand that it is impossible to apprehend them. Additionally, some recommendations for preventing crime are given. Knowing the different types of cybercrime and the basic preventative measures can help internal auditors evaluate if a company has adequate cybercrime defenses. The author discusses cybercrimes, their various varieties, and preventative measures in this study. This paper will discuss cybercrimes and possible preventative measures in the future.

REFERENCES:

[1] D. A. Akopyan and A. D. Yelyakov, “Cybercrimes in the information structure of society: A survey,” *Sci. Tech. Inf. Process.*, 2009, doi: 10.3103/S0147688209060057.

[2] R. Sabillon, J. Serra-Ruiz, V. Cavaller, and J. J. Cano, “Digital Forensic Analysis of Cybercrimes,” *Int. J. Inf. Secur. Priv.*, 2017, doi: 10.4018/ijisp.2017040103.

[3] A. Hassan, “Cybercrime in Nigeria: Causes, Effects and the Way Out,” *ARPN J. Sci. …*, 2012.

[4] E. R. Leukfeldt and M. Yar, “Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis,” *Deviant Behav.*, 2016, doi: 10.1080/01639625.2015.1012409.

[5] S. R. Kim, J. H. Yang, and S. B. Kim, “A cybercrime prevention program based on simulation and quiz game: Applying item response theory for effective information security learning,” *Int. J. Secur. its Appl.*, 2016, doi: 10.14257/ijsia.2016.10.5.16.

[6] O. Enigbokan and N. Ajayi, “Managing Cybercrimes Through the Implementation of Security Measures,” *J. Inf. Warf.*, 2017.

[7] F. E. Eboibi, “A review of the legal and regulatory frameworks of Nigerian Cybercrimes Act 2015,” *Comput. Law Secur. Rev.*, 2017, doi: 10.1016/j.clsr.2017.03.020.

[8] E. R. Leukfeldt, A. Lavorgna, and E. R. Kleemans, “Organised Cybercrime or Cybercrime that is Organised? An

Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime," *Eur. J. Crim. Policy Res.*, 2017, doi: 10.1007/s10610-016-9332-z.

[9] E. F. G. Ajayi, "Challenges to enforcement of cyber-crimes laws and policy," *J. Internet Inf. Syst.*, 2016, doi: 10.5897/jiis2015.0089.

[10] A. A. S. Al Hait, "Jurisdiction in cybercrimes: A comparative study," *J. Law Policy Glob.*, 2014.

[11] B. Omodunbi, P. Odiase, O. Olaniyan, and A. Esan, "Cybercrimes in Nigeria: Analysis, Detection and Prevention," *FUOYE J. Eng. Technol.*, 2016, doi: 10.46792/fuoyejet.v1i1.16.

[12] E. Tambo, "Promoting cybersecurity awareness and resilience approaches, capabilities and actions plans against cybercrimes and frauds in Africa," *Int. J. Cyber-Security Digit. Forensics*, 2017, doi: 10.17781/p002278.

[13] M. Levi, "Assessing the trends, scale and nature of economic cybercrimes: overview and Issues: In Cybercrimes, Cybercriminals and Their Policing, in Crime, Law and Social Change," *Crime, Law Soc. Chang.*, 2017, doi: 10.1007/s10611-016-9645-3.

[14] D. Mohamed, "Investigating cybercrimes under the Malaysian cyberlaws and the criminal procedure code: issues and challenges," *Malayan Law J.*, 2012.