A Recent Survey on Cybercrime and Its Defensive Mechanism

Garima Bajaj, Saurabh Tailwal, and Anupama Mishra

Abstract Cybercrime is one of the severe issues in today's world that is increasing day by day due to unawareness of people about the harm it can cause. The main reason against the augmentation of cybercrime is the lack of education or knowledge about the impact it can lead to. Cybercrime can be done against individuals, society, or any organization whether it is private or government. The aim of the paper is to focus on what cybercrime is, its types, related work, and its defensive mechanism. Defensive mechanism against cybercrime includes the ways or measures that how can any individual or any organization protects them against cybercrime. This paper also includes the related work which includes some points about the work which has been done so far on cybercrime.

Keywords Cyber security · Cyber crime · Phishing · Cyber stalking · Social engineering

1 Introduction

The word cybercrime is the combination of two words cyber + crime which means the crime related to computer or the things related to it. Cybercrime is the crime that can be caused by the involvement of computer, network, or any network device. Cybercrime can be carried out by a particular individual or by big organization. A hacker hacking any person's data or the data of any organization for his/her profit is also a part of cybercrime. Stealing someone's pictures without his/her permission and using it badly just in order to satisfy revenge is also a part of cybercrime. There are tremendous amount of examples of cybercrimes in India. In India, cybercrime is increasing day by day because the use of Internet or you can say the number of Internet users is increasing day by day due to lack of understanding about cybercrime or about the impact it can cause. The misuse of Internet is spreading in India which

G. Bajaj (✉) · S. Tailwal · A. Mishra
Swami Rama Himalayan University, Dehradun, India
e-mail: garimabajaj9818@gmail.com

D. P. Agrawal et al. (eds.), *Cyber Security, Privacy and Networking*, Lecture Notes in Networks and Systems 370, https://doi.org/10.1007/978-981-16-8664-1_29

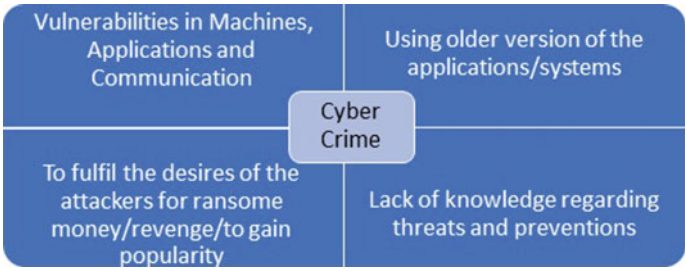

Fig. 1 Causes of cybercrime

in turns increases the rate of cybercrime. Our daily lives are replete with information technologies that we rely on to simplify our lives. In today's environment, mobile phones, the Internet, and email have become indispensable for communication. Every common man is familiar with the terms "hacker" and "virus," which are frequently used in conjunction with data loss, sophisticated theft of money, and compromised security. Cybercrime is becoming increasingly prevalent these days [1] (Fig. 1).

2 Related Work

Cybercrime is defined as crimes committed using a communication channel or device, whether it is a laptop, desktop, PDA, mobile phone, watch, or vehicle, directly or indirectly. According to the report, titled "Global Risks for 2012," cyberattacks will be one of the top five risks to the world's governments and businesses in 2012. Cybercrime is a type of crime that is more difficult to detect and harder to stop once it has occurred, resulting in long-term negative consequences for victims [2]. Although the concept of cybercrime is not new, there is considerable confusion among academics, computer security experts, and users regarding the scope of true cybercrime. We examine the breadth of computer-based crime in this article, including a definition of the emerging terms "cybercrime" and "crimeware." Then, we categorize cybercrime into two distinct categories: Type I Cybercrime, which is primarily technological in nature, and Type II Cybercrime, which has a stronger human component. Then, using two case studies, we demonstrate the role of crimeware in various types of cybercrime and make some observations about the role of cognition in the cybercrime process [3].

3 Classification of Cybercrimes

Cybercrimes can be categorized based on many perception like based on criminal behviour, based on crime type, based on size of the target like individual/organization/society.

3.1 Cybercrimes Based on Target Size

Cybercrimes are divided into three main groups.

(1) Cybercrime against individuals—The type of cybercrime which is done against a particular person or against people. It includes:

- Email harassment
- Spoofing with email
- Cyberstalking
- Unauthorized access
- Fraud.

(2) Cybercrime against organization—The type of cybercrime which is done against any organization whether it is government or private or any other company. It includes:

- Retrieval of unauthorized information
- Cyber terrorism
- Hacking of organization's server
- Distribution of pirated software.

(3) Cybercrime against society—The type of cybercrime which is done against society. It includes:

- Trafficking
- Gambling
- Forgery
- Spoiling the youth with filthy material.

3.2 Cybercrimes Based on Crime

(1) Forgery—When an offender alters documents stored in a computerized form, the crime associated with it is known as forgery. In this computer systems are the target to carry out such criminal activities.

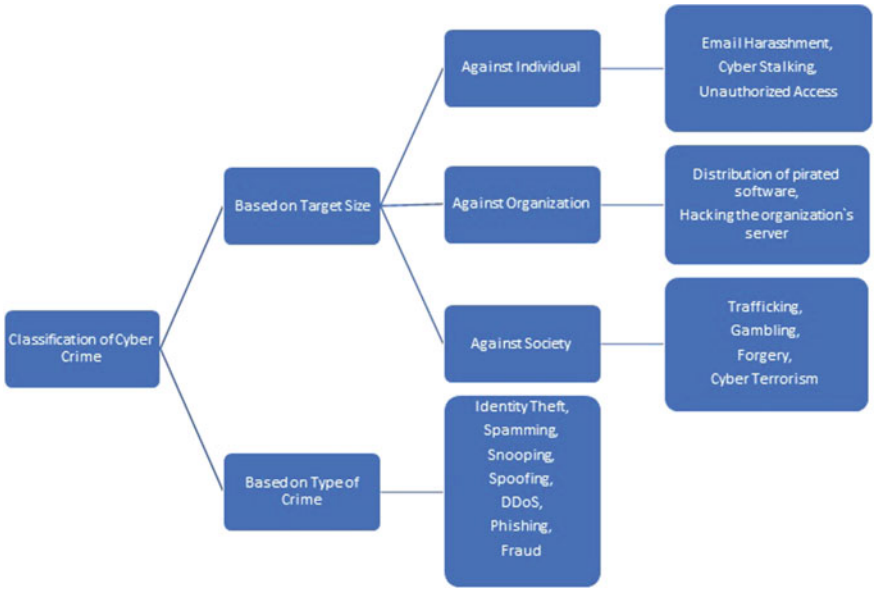

Fig. 2 Classification of cybercrime

(2) Email spoofing—It is referred to as crime in which sender sends the fake mails to the receiver. In this origin, details have been altered so as to make it appear that it originates from other source. It is used to launch phishing attacks [4].
(3) Cyberstalking—It refers to the use of email, Internet to commit criminal activity which includes harassment of victims without the victim's permission, and in this way, the criminal can create fear in victim. Cyberstalking is ignited by rage, power, control, and anger that have been triggered by victim's action or in many cases victim's inactions [5].
(4) Hacking—It is the art of solving problem in a creative manner that means finding an uncommon solution to a hard problem or manipulating holes in an unsystematic programming [6].
(5) Cyber terrorism—Cyber terrorism is defined as the use of computer network tools to close down critical national infrastructures such as government operations [7].
(6) Phishing—Phishing is a form of attack in which an attacker aims to acquire sensitive information from a victim by portraying itself as a reliable entity [8].
(7) Fraud—Fraud is increasing worldwide with the increase in use of modern technology resulting in the loss of billion dollars throughout the world. Fraud includes credit card fraud, telecommunication fraud, etc. [9].
(8) Gambling—Gambling can occur almost in all cultures and in every period of time. It refers to risk taking activities. It can be understood as staking of money, investment in stock market. It allows an individual or group of organizations to extract profit [10] (Fig. 2).

4 Defensive Mechanisms Against Cybercrime

4.1 Information Assurance

To protect our information, there are five basic principles:

(1) Confidentiality—Confidentiality means to keep the information or data confidentiality and can only be accessible to authorized users. Only authorized users can copy and use that information. For example, you give permission to someone for viewing the information who is not authorized, but the authorized user is allowed to completely access it.
(2) Integrity—Data integrity means to maintain the integrity of data where an unauthorized user is not allowed to alter or delete data. Data integrity can occur when our computer is attacked by the virus or when hacker gains unauthorized access to our server and can delete and modify our important data.
(3) Authenticity—It means that the user should be an authorized person who has his own credentials like username and password and documents of the users cannot be altered without user's permission.
(4) Availability—Availability means that the information should be available to the authorized users and the measures to protect the file can be properly taken to protect it and will make sure that the exact information should be available to a correct person.
(5) Non-repudiation—Non-repudiation means the guarantee that the person cannot deny the validity of something. It assures that there are enough evidences that the person cannot deny over something.

4.2 To Implement Defense in Deep Plan of Action

- To broaden organizational boundaries: Businesses today maintain tight ties with their business partners, consumers, and suppliers. This results in difficult-to-define exterior boundaries; for example, when business partners join an association for the purpose of delivering a product, it is because they share the same infrastructure, computer systems, and personnel. It is critical to define the organization's boundaries and how it is implementing its defense in depth plan.
- Mobile workforce: It is critical for employees to be capable of accessing their company's network from a remote place. Employees must have access to the same software applications and data as those at the corporate headquarters. This interconnection enables viruses and hackers to spread throughout the system, causing damage.
- Decentralization of services: As there is increase in the use of computers at workplace, on the other hand, there is increase in the services. Earlier these services are provided to a limited amount of users, but now, they are provided to a broad

category of users. As from business point of view, the business information is very important, so it will be a prime responsibility to protect this information from unauthorized access, and in this way, it may assist in achieving good governance and improves in delievery of service.

The steps for implementing defense in deep plan of action

- Internal and external environment analysis: This is the foremost step for implementing defense in deep plan of action. It is very important for an organization to check internal and external environment in which it is operating. It should be very important for an organization to know about its strengths and weakness and what are the threats an organization will going to face and what technology and processes are being used. It is also very important for an organization to properly strategize about defense plan in action and clearly understands about the steps to implement defense in deep plan of action.
- Determining the risks: This is the second step which determines the risks which an organization will face. It includes the threats and vulnerabilities. It is necessary for an organization to identify risk and will take proper measures to reduce these risks. An organization should always be ready for such risks and with proper mitigation steps.
- Strategy of defense in-depth implementation: If all risks have been identified properly, then now it comes to deal with such risks with proper pre-planned strategy and will make use of proper defense mechanism.
- Maintenance, monitoring, and review: As we all know that technology is increasing day by day so the risk of threats and risks are also increasing so it very important to properly monitor, maintain, and review all this and will adapt the changes accordingly [11].

4.3 Education

It is one of the most important defensive mechanisms. People should be educated about the harmful impact of cybercrime. They should be aware of the punishments which are there under the IT Act about the offence off cybercrime committed by them. They should be aware of the do's and don't over the Internet. People should know that following someone and using other people's private information is also a part of cybercrime (Fig. 3).

5 Conclusion

The objective of this paper is to spread awareness about what cybercrime is and what are its types. In this paper, we have studied about existing definition and work about cybercrime, and following this, we have added definition of cybercrime according

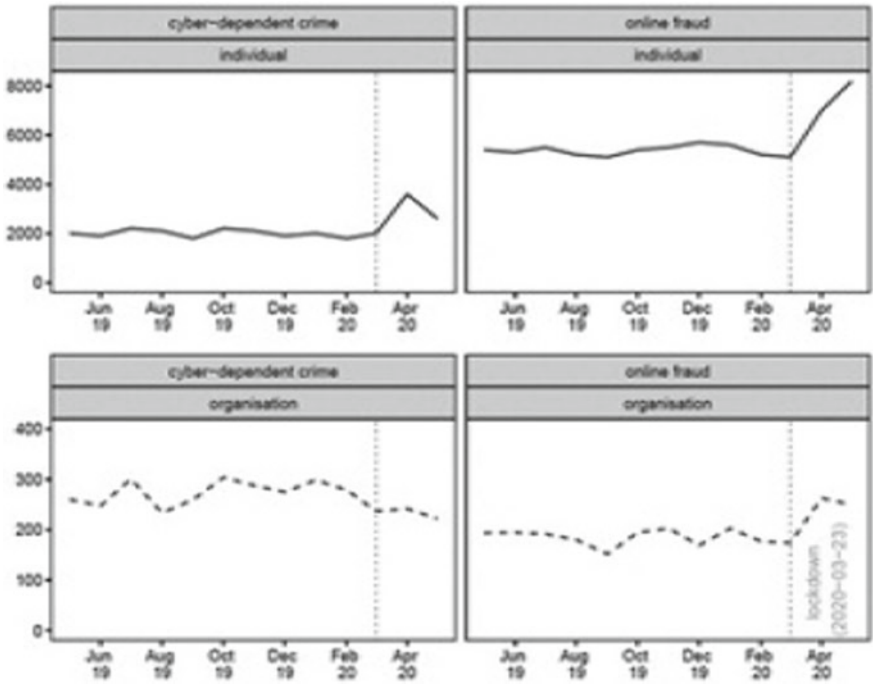

Fig. 3 Cybercrime statistics

to our understanding. Types of cybercrimes have been also added based on present scenarios. With the help of our increased understanding about the types of it, many people can be solved from becoming a part of cybercrime. Finally, we conclude that understanding about cybercrime is very important and spreading awareness about the impact of it is very important. By studying about the defensive mechanism of cybercrime, we can reduce the rate of cybercrime.

References

1. Furnell S (2002) Cybercrime: vandalizing the information society. Addison-Wesley, London, pp 3–540
2. Gunjan VK, Kumar A, Avdhanam S (2013) A survey of cyber crime in India. In: 2013 15th international conference on advanced computing technologies (ICACT), Sept 2013. IEEE, pp 1–6
3. Gordon S, Ford R (2006) On the definition and classification of cybercrime. J Comput Virol 2(1):13–20
4. Pandove K, Jindal A, Kumar R (2010) Email spoofing. Int J Comput Appl 5(1):27–30
5. Pittaro ML (2007) Cyber stalking: an analysis of online harassment and intimidation. Int J Cyber Criminol 1(2):180–197
6. Erickson J (2008) Hacking: the art of exploitation. No Starch Press

7. Lewis JA (2002) Assessing the risks of cyber terrorism, cyber war and other cyber threats. Center for Strategic & International Studies, Washington, DC, p 12
8. Jagatic TN, Johnson NA, Jakobsson M, Menczer F (2007) Social phishing. Commun ACM 50(10):94–100
9. Bolton RJ, Hand DJ (2002) Statistical fraud detection: a review. Stat Sci 17(3):235–255
10. McMillen J (1996) Understanding gambling. In: Gambling cultures: studies in history and interpretation, pp 6–42
11. Fick J (2009) Prevention is better than prosecution: deepening the defence against cyber crime. J Digit Forensics Secur Law 4(4):3
12. Buil-Gil D, Miró-Llinares F, Moneva A, Kemp S, Díaz-Castaño N (2020) Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. Eur Soc 1–13
13. Mishra A, Gupta N, Gupta BB (2020) Security threats and recent countermeasures in cloud computing. In: Modern principles, practices, and algorithms for cloud security. IGI Global, pp 145–161
14. Mishra A, Gupta N (2019) Analysis of cloud computing vulnerability against DDoS. In: 2019 international conference on innovative sustainable computational technologies (CISCT), Oct 2019. IEEE, pp 1–6
15. Bhushan K, Gupta BB (2019) Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. J Ambient Intell Humaniz Comput 10(5):1985–1997
16. Alsmirat MA et al (2019) Impact of digital fingerprint image quality on the fingerprint recognition accuracy. Multimed Tools Appl 78(3):3649–3688
17. Dahiya A, Gupta BB (2020) Multi attribute auction based incentivized solution against DDoS attacks. Comput Secur 92:101763
18. Al-Qerem A et al (2020) IoT transaction processing through cooperative concurrency control on fog cloud computing environment. Soft Comput 24(8):5695–5711
19. Gupta S, Gupta BB (2015) PHP-sensor: a prototype method to discover workflow violation and XSS vulnerabilities in PHP web applications. In: Proceedings of the 12th ACM international conference on computing frontiers, May 2015, pp 1–8
20. Dahiya A, Gupta BB (2020) A reputation score policy and Bayesian game theory based incentivised mechanism for DDoS attacks mitigation and cyber defense. Future Gener Comput Syst