GLOBUS

Globus An International Journal of Medical Science, Engineering and Technology
A Refereed Research Journal
Vol 11 / No 1 / Jan-Jun 2022 ISSN: 2319-8958

EXPLORATION AND MECHANISMS OF CYBER CRIME OPERATIONS

*Divya Sharma
**Dr Atal Kumar

Paper Received: 16.06.2022 / **Paper Accepted**: 31.07.2022 / **Paper Published**: 09.08.2022
Corresponding Author: Divya Sharma; Email: divyasharma260.ds@gmail.com; doi:10.46360/globus.met.320221020

Abstract

This study discusses about study and functioning of cyber crime. Cybercrime attacks can begin wherever there's digital data, opportunity and motive. Cybercriminals include everyone from the lone user engaged in cyber bullying to state-sponsored actors, like China's intelligence services. Cybercrimes generally don't occur during a vacuum; they're, in some ways, distributed in nature. That is, cybercriminals typically believe other actors to finish the crime. This is often whether it is the creator of malware using the dark web to sell code.

Keywords: Cyber Crime, Cybercriminal, Technology, Cyberattack, Cybersecurity.

Introduction

The operation of cybercrime is a complex and ever-evolving process that takes advantage of vulnerabilities in digital systems and networks for the purpose of committing destructive acts. It starts with the identification of potential targets, which can range from individuals to huge organisations. This identification is typically based on perceived value or susceptibility to attack against the target. Then, in order to acquire unauthorised access, cybercriminals will use a variety of methods to exploit vulnerabilities. These methods may include exploiting software faults, utilising weak passwords, or employing social engineering strategies such as phishing.

After successfully gaining access to a system or network, fraudsters establish a footing and may then implant malware in order to either maintain their access or steal sensitive data. Cybercriminals frequently target financial information, intellectual property, or personal records for the intention of obtaining financial gain or other nefarious motives. Data theft and manipulation are common objectives for cybercriminals. Cybercriminals are able to monetize their activities by selling stolen data on underground markets, conducting fraudulent transactions, or extorting victims through ransomware attacks since the internet provides anonymity, which makes it easier for them to gain financial gain.

Cybercriminals adopt many methods to avoid discovery and attribution, which is an essential component of their activities. Covering their tracks is a vital feature of cybercrime operations. This involves the removal of logs, the concealment of digital footprints, and the utilisation of technology that provide anonymization, such as virtual private networks (VPNs). Defenders face constant problems as a result of the ongoing evolution of cybercrime methods, which is driven by advancements in technology and security measures.

In order to effectively combat cybercrime, a coordinated approach is required. This approach

* *Research Scholar, Himalayan Garhwal University, Shiv Nagar, Phokra, India.*
***Research Supervisor, Himalayan Garhwal University, Shiv Nagar, Phokra, India.*

should include technical restrictions, awareness campaigns, legislative frameworks, and international cooperation. When stakeholders have a greater grasp of how cybercrime operates, they are better able to foresee potential threats, put into action effective responses, and work towards creating a digital ecosystem that is more resilient.

Review of Literature

Showkat (2020) [1] The Internet is transforming into the town square of the forthcoming global village. The Internet has linked every individual as if they were neurons in a gigantic brain. The internet has become both an asset and a bane for modern society. At this moment. Furthermore, in light of the expanding utility of the internet, safeguarding our data and information has become an absolute necessity. Whether you are an individual user of the internet or a proprietor of a company or business, it is imperative that you understand how to mitigate threats, risks, and cybercrime.

Additionally, you should exercise prudence, proactivity, and remain updated on cybercriminals. Because of technological progress, man now relies exclusively on the Internet to fulfil his requirements. MAN, now has simple access to everything from a single location, thanks to the Internet. Various activities such as social networking, online purchasing, data storage, gaming, studying, and working remotely are all conceivable and can be accomplished via the internet. Internet usage permeates virtually every domain. The emergence of the internet as well as its associated advantages coincided with the emergence of the cybercrime concept. Cybercrimes manifest in a variety of ways. A few years ago, there was a dearth of knowledge regarding the potential for criminal activities to be executed via the internet.

With regard to cybercrimes, India is not lagging behind other nations in which the incidence rate of such crimes is progressively escalating. Based on the most recent government data, cybercrime cases in India have increased by a significant 63.5% in 2019. According to data from the National Crime Record Bureau (NCRB), the number of reported cybercrime incidents in 2019 rose to 44,546 from 28,248 in 2018. Karnataka recorded the greatest quantity of cybercrime cases (12,020), with Uttar Pradesh (11,416), Maharashtra (4,967), Telangana (2,691), and Assam (2,231) following suit in that order. Cybercrime in the Union Territory of Delhi was responsible for 78% of the total.

Anupreet (2017) [4] Internet usage for routine transactions has become an integral part of the majority of people's daily lives. As the amount of people using the internet has increased dramatically, so has the incidence of cybercrimes. Cybercrime is the commission of an offence through the use of a computer or network. Cybercrime is a persistent and escalating menace that affects both the private as well as public spheres. As a result of the introduction of the internet, classic crimes have assumed a new form.

The objective of this study is to raise awareness about the prevalence of cybercrimes in the contemporary world and to promote greater cyber security. The objective of this study is to examine the level of cyber-crime awareness among internet consumers across various age cohorts and educational backgrounds. The linear regression model was utilised to examine both of the objectives. This study demonstrates that a correlation can be observed between the educational attainment of the participants and the age divisions of the participants.

Therefore, it is the responsibility of every internet user to be informed about cybercrime and security and to assist others in doing the same by spreading awareness. The internet is expanding swiftly in India. It has generated novel prospects across various sectors, including but not limited to entertainment, business, athletics, and education. The proliferation and ever-growing utilisation of the internet has enabled businesses to transcend the limitations imposed by local markets and establish connections with consumers across the globe. Computers are extensively employed within organisations for purposes beyond information processing; they are also utilised to obtain a competitive and strategic edge.

There are both constructive and destructive applications for computers. The emergence of new age crimes, which have been addressed through the Information Technology Act of 2000, can be attributed to the misuse of the internet. As the accessibility of information has increased on a global scale, it has concurrently become more susceptible to misuse. India has become a target of cybercriminals due to the increasing frequency of cyberattacks against Indian institutions. India is positioned third in terms of pernicious activity originating from the internet, following the United States and China. It ranks second in terms of malicious code as well as fourth and eighth, respectively, in terms of web and network attacks.

Analysis

Cybercriminals use various attack vectors to hold out their cyber attacks and are constantly seeking new methods and techniques for achieving their goals, while avoiding detection and arrest. Cybercriminals often perform their activities using

malware and other sorts of software, but social engineering is usually a crucial component for executing most sorts of cybercrime. Phishing emails are another important component to several sorts of cybercrime but especially so for targeted attacks, like business email compromise (BEC), during which the attacker attempts to impersonate, via email, a business owner so as to convince employees to disburse bogus invoices. The operation of cybercrime is comprised of a variety of processes and methods that are conducted with the intention of exploiting vulnerabilities in digital systems and networks for the purpose of committing hostile acts. The following is an outline of the typical operational procedures of cybercrime:

1. Target Identification: Cybercriminals identify possible targets, which may include individuals, organisations, or even entire networks. Targets can be identified in a number of different ways. It is possible that they will employ automated programmes to search the internet for susceptible systems or that they will explicitly target businesses based on factors such as perceived value, inadequate security measures, or personal information.

2. Vulnerability Exploitation: Once a target has been discovered, hackers will exploit vulnerabilities in software, hardware, or human behaviour in order to gain unauthorised access to the target. In this context, exploiting refers to exploiting software vulnerabilities, misconfigurations, weak passwords, social engineering tactics (such as phishing), or utilising known security weaknesses.

3. Infiltration and Access: Once they have gained initial access, hackers will then establish a foothold within the system or network that they are attempting to compromise. In order to accomplish their goals of maintaining persistence, stealing sensitive data, or using the hacked machine as a launching pad for additional attacks, they may employ malicious software (such as viruses, ransomware, or trojans).

4. Theft or manipulation of data: Cybercriminals frequently target important data, such as financial information, intellectual property, personal details, or login credentials with the intention of stealing or manipulating it. They may steal this information for a variety of malicious reasons, including financial gain, espionage, identity theft, and other illegal activities. It is possible that they will falsify data in order to disturb operations, cause financial damage, or propagate false information in some instances.

5. Monetization: The pursuit of financial gain is the driving force behind many cybercrimes. It is possible for cybercriminals to get revenue from stolen data by selling it on underground marketplaces, extorting victims through ransomware attacks, engaging in fraudulent transactions, or engaging in other illegal acts. Internet anonymity and the internet's ability to reach people all over the world make it simpler for them to avoid detection and to clean their money.

6. Covering Tracks: In order to avoid being discovered and attributed, cybercriminals frequently cover their tracks by erasing records, concealing their digital footprint, or employing anonymizing technologies such as virtual private networks (VPNs) or the Tor network. In addition, they can use anti-forensic measures in order to make it more difficult for investigators to reconstruct the activities that they were involved in performing.

7. Continual Evolution: It is important to note that cybercrime strategies are always evolving as a result of technology breakthroughs, security measures, and the activities of law enforcement. To maintain a competitive advantage over defenders and to maximise their unlawful gains, cybercriminals are constantly adapting their techniques, taking advantage of newly discovered weaknesses, and investigating future technology (such as artificial intelligence or cryptocurrencies).

In order to effectively combat cybercrime, a multi-pronged approach is required. This approach should include technical restrictions, awareness and education, legal frameworks, international cooperation, and coordination between the public and private sectors. Stakeholders are able to better predict risks, adopt effective countermeasures, and work towards a safer and more secure digital environment if they have a better grasp of the working of cybercrime.

Conclusion

The study of cybercrime exposes a complicated world where the quick development of technology presents both chances for creativity and susceptibilities to abuse. Identity theft and cyberterrorism are just two examples of the many nefarious acts that fall under the umbrella of cybercrime, which presents serious obstacles to people, businesses, and countries alike. Through this inquiry, we have learned about the complex mechanisms behind cybercrime, which take use of

the internet's wide reach and anonymity to carry out sophisticated cross-border attacks with little chance of detection.

Important discoveries show that cybercriminals frequently take use of flaws in human psychology, software, and systemic vulnerabilities in our digital infrastructure. Because social engineering is intricately entwined with the technical functioning of cybercrime, it poses a persistent danger that necessitates a multifaceted approach to both prevention and response.

Cybercrime has a significant impact on the social, political, and economic spheres. There are annual losses in the billions of dollars, but a more subtle effect is the deterioration of public confidence in digital platforms and organisations. The study has also highlighted the dynamic character of cyber threats, which change quickly to elude security precautions and take advantage of emerging technologies.

In order to reduce the likelihood of cybercrime, preventive measures such as strong cybersecurity standards, public awareness campaigns, & international cooperation are essential. It is impossible to overestimate the importance of legal frameworks, which is why new laws are required to reflect the complexity of the digital age and to make international cooperation in the fight against cybercrime easier.

Nonetheless, there are several obstacles in the way of the battle against cybercrime. The internet's anonymity, legal concerns regarding jurisdiction, and the ever-changing nature of cyberthreats provide significant challenges to both prevention and prosecution. Furthermore, the digital gap emphasises how different countries are able to combat cybercrime, underscoring the necessity of international cooperation in combating this pervasive menace.

Future efforts to combat cybercrime will need to focus on developing an international legal & cooperative framework that is flexible enough to respond to the always evolving threat landscape. This will be in addition to requiring technological innovation. People will be able to defend themselves in the digital environment with the help of education and awareness. Our methods for preserving the integrity of our digital lives against the threat of cybercrime must also develop along with technology.

The research on cybercrime emphasises how urgent it is to tackle cybersecurity from a global, comprehensive perspective. It asks for coordinating initiatives by the public, commercial, & civil society sectors in order to promote a safer online environment. As the digital era deepens, our societies' ability to withstand cyberattacks will become increasingly important to our overall security and well-being.

Conflicts of Interest

The authors declare there are no significant competing financial, professional, or personal interests that might have influenced the performance or presentation of the work described in this manuscript.

References

1. Showkat Ahmad Dar and Lone, Dr. Naseer Ahmad (2020). Cyber Crime in India. Sambodhi, 43(4) (VIII), 118-130.
2. Fennell, C. and Wash, R. (2021). Do Stories Help People Adopt Two-Factor Authentication? https://www.rickwash.com/papers/SOUPS2019_LBW_Submission.pdf (accessed on 30 April 2021).
3. Al-Khater, W.A., Al-Maadeed, S., Ahmed, A.A., Sadiq, A.S. and Khan, M.K. (2020). Comprehensive Review of Cybercrime Detection Techniques. IEEE Access, 8, 137293-137311.
4. Mokha, Anupreet Kaur (2017). A Study on Awareness of Cyber Crime and Security. Research J. Humanities and Social Sciences, 8(4), 459-464. doi: 10.5958/2321-5828.2017.00067.5
5. Tonge, Atul M., Kasture, Suraj S. and Chaudhari, Surbhi R. (2013). Cyber security: challenges for society-literature review. IOSR Journal of Computer Engineering (IOSR-JCE), 12(2), 67-75.
6. Aljeaid, D., Alzhrani, A., Alrougi, M. and Almalki, O. (2020). Assessment of End-User Susceptibility to Cybersecurity Threats in Saudi Arabia by Simulating Phishing Attacks. Information, 11, 547.