A Survey on Crime Prevention Using Cyber Security

Vishwanath V Murthy
MCA Department
RNS Institute of Technology
Bengaluru, India
Mail: vishwanathmurthy@rnsit.ac.in

G. Ananya Datt Revankar
MCA Department
RNS Institute of Technology
Bengaluru, India
Mail: mca.ananyadattrevankar@gmail.com

Inchara S M
MCA Department
RNS Institute of Technology
Bengaluru, India
Mail: mca.incharasm@gmail.com

Deepak Kumar CV
MCA Department
RNS Institute of Technology
Bengaluru, India
Mail: mca.deepakkumarcv@gmail.com

Darshan P
MCA Department
RNS Institute of Technology
Bengaluru, India
Mail: mca.darshanp@gmail.com

***Abstract*—Criminologists and Crime deterrence practitioners identifies the critical role that geographical locations play in criminal activities and the potential of place managers to effectively prevent crime. Over the past several decades, extensive research has demonstrated the tendency for crime to cluster in certain geographic areas, often where place management is lacking or ineffective. However, there has been limited research on evaluating place management strategies and cybercrime in the virtual realm. This study aimed to assess the effectiveness of place management techniques in reducing cybercrime incidents online. Using data from the information technology division of a large urban research university in the United States, the study evaluated the impact of an anti-phishing training program delivered to employees. This program aimed to increase awareness and understanding of methods to better protect their ”virtual places” from cybercrimes. The findings are discussed within the broader context of crime and place literature.**

***Index Terms*—Cybercrime, Crime prevention**

I. Introduction

Cybercrime encompasses criminal activities that target or utilize computers, computer networks, or networked devices. While profit is the primary motivation for most cybercrimes, there are instances where the goal is to disrupt or damage computers or networks for reasons other than financial gain, such as political or personal agendas.

Cybercrime encompasses activities carried out by individuals or groups. Some cybercriminals operate in organized factions, utilizing advanced methods and showcasing significant technical prowess. Conversely, there are also less skilled hackers involved in cybercrime.

II. Applications

A. DDOS Security

DDoS stands for Distributed Denial for Service attack. The attacker here has used numerous devices to keep the web server engaged by accepting the requests which were sent by him from the multiple devices. This creates a fake website traffic on the server. To counter, Cybersecurity helps to allocate DDoS mitigation service, which helps counter it by diverting the same to other cloud-based servers, thus rescuing the situation.

B. Web Firewall

A large area network contains a firewall based on a web application server, which applies and examines all the incoming and outgoing traffic on the server and automatically traces and removes the traffic on the fake and malicious website. This cybersecurity helps to determine and enables auto traffic monitoring hence reducing the risk of the attack.

C. Bots

In the modern computing world, many hackers or attackers use bots to generate traffics of many devices on the server, which causes it to crash. Cybersecurity helps resolve the identification of fake users—that is, bots—and makes them log out of their sessions so as not to disrupt the experience of normal users.

D. Antivirus and Anti malware

It develops antivirus and antimalware software, thus helping cybersecurity to prevent all possible digital attacks on a computer or device from data breaches and digital attacks to unauthorized attacks by hackers. This also aids in maintaining network securities and firewall systems concerning all connected devices on the network.

E. Threat management systems

Cybersecurity deals with the digital risks and attacks by finding the weaknesses and faults in the computer system that hackers and attackers may use. It optimizes automatically those weaknesses, thus improving the performance of the system. It enhances the power to come up quickly from a digital attack and provides effective control to the users regarding the issues of vulnerability.

F. Critical systems

Cyber security helps deal with the critical issue of incursions that are undertaken onto large servers connected to wide-area networks. It does maintain the standard high safety protocols to ensure that users do conform to the rules of cybersecurity to protect their devices. All applications are monitored in real-time, and it checks, periodically, the safety of the servers, the network used by it, and the users themselves.

G. Rules and regulations

Cybersecurity makes new rules and regulations for the users, attackers, and people on the network to follow and comply with certain rules and norms while using the Internet. This gives power to the authorities to investigate security issues and optimize the network accordingly.

III. What is Cyber Security?

Cybersecurity entails protecting computer systems, networks, and data from malicious activities such as hacking, phishing, and other cyber threats. The aim of cyber attacks is to,

1) **Unauthorised or illegal access to data:** Accessing data for the purpose of either modifying or deleting it.
2) **Extortion:** Illegally accessing private and sensitive data to extort money from the victim.
3) **Hurt the Competition's Business:** Stealing trade secrets or valuable intellectual property can severely damage a competitor's business by diminishing their financial value and impacting overall profitability.
4) **Disrupt Business activity:** One objective of cyber attacks is to disrupt the daily operations of an organization.
5) **Damage reputation:** Sometimes organisations may experience security breaches, and although their impact would be minimal, they could damage the organisation's reputation among the public.

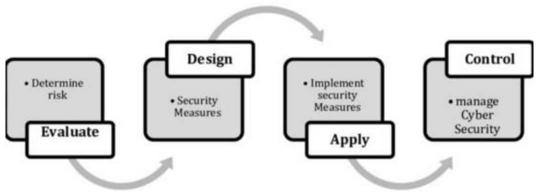

Fig. 1. Cyber Security Process

IV. Emergence of Cyber Threat Management

The first ever recorded cybercrime is believed to have happened in 1820. This shows that crimes on computing technologies have been here since their invention in India, China, and Japan dating as far back as 3500 BC. Other than the analytical engine of Charles Babbage, there was some other invention of computing technology.

V. Legislation for Cyber Defense

The government's obligation is to ensure that its laws adapt to the progress of science and technology, and to actively participate in legislative activities.

- The IT Legislation of 2000 in India
- RA 8792: The Philippines Electronic Commerce Act of 2000
- RA 10175: The Philippines Cybercrime Prevention Act of 2012
- The 2011 USA Cyber Intelligence Sharing and Protection Act (CISPA)
- The 2009 Cyber Security Enhancement Act in the United States

VI. Advantages

All these years make the world significantly safe from rapists, pedophiles, and other kinds of criminals due to the fact that everything can be found as long as it's online.

- *Rise in Cyber Defence:* Since every cybercrime is invented by finding a new loophole, it keeps the people working on the systems for defense on their toes to improve and evolve continuously.
- *Safeguard sensitive personal information:* Today, data is considered an asset in the utmost sense of the term. It becomes even more crucial when the data under consideration contains personal information. Blackmailing or marinating the character of a person is very possible if hackers access a person's data illegally; therefore, Cyber Security will successfully prevent such attacks in the first place because it is a proactive approach.
- *Private and Business data Protection:* It is an absolute security package. It can save businesses and organizations from many threats. For example, companies have to protect sensitive data like Intellectual Property, trade secrets, other private information like their internal communication logs. Cyber-security can protect an organization then very effectively with its constant monitoring and detection of entities well in advance.

VII. Disadvantages

- *Regular Update:* It's essential for businesses to regularly update their software, hardware, and security strategy to maintain a proactive stance against attackers.

- *Needs Continuous learning:* The threats are relentless and always changing, demanding a continuous learning process to stay vigilant.

- *Expensive:* Deploying cybersecurity measures is expensive, involving ongoing learning and financial outlays, which can strain many small businesses.

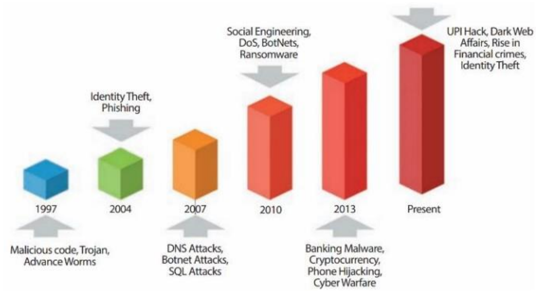

Fig. 2. Drone Visualization

VIII. Evolution of Cybercrime

The first cybercrime dates back to 1997, coinciding with the internet's development. Initially, cybercrimes were rudimentary, involving the theft of information from local computers or networks through methods like Flash memory or floppy drives. As the internet became indispensable globally, cybercrimes evolved from local networks to encompass the entire internet.

IX. Conclusion

Historical studies and records clearly indicate that technological advancements coincide with an increase in cybercrimes. It's striking that cybercrimes are predominantly carried out by skilled individuals, emphasizing the importance of understanding basic internet ethics and principles.

Cybercrimes and hacking pose substantial threats to internet safety. Drawing lessons from past incidents, we can employ diverse strategies to mitigate cybercrime. Swift adaptation of cyber laws is crucial for effectively combating cybercrime, responding swiftly like hackers while maintaining a balance between protecting citizens and upholding their rights.

Despite the vastness and freedom of the internet, questions persist about its ability to enforce strict measures against cyber offenders. While the Indian government has taken steps to reduce cybercrimes and promote safe internet usage, cyber laws must remain dynamic, evolving in step with technological progress.

References

[1] Ms M Lakshmi Prasanthi, Tata A S K Ishwarya-2015 Cyber Crime: Prevention and Detection

[2] Chandra Sekhar Biswal and Dr.Subhendu Kumar Pani -2020 Cybercrime prevention Methodology

[3] Abhishek Anand, Abhijit Chirputkar, P. Ashok, ”Addressing Cybersecurity Risks through Cyber Analytics,” -2023

[4] Andrew Ishmael, Dr. Leila Halawi, ”Retaining Qualified Cybersecurity Professionals: A Qualitative Study,” published in the Journal of Computer Information Systems, vol. 63, no. 1, pp. 204, 2023.

[5] Michael Veale, Ian Brown, ”Cybersecurity”, Internet Policy Review, vol.9, no.4 -2020.

[6] Bryan Irvin Lamarca, ”Cybersecurity Risk Assessment of the University of Northern Philippines using PRISM Approach”, IOP Conference Series: Materials Science and Engineering, vol.769 -2020.