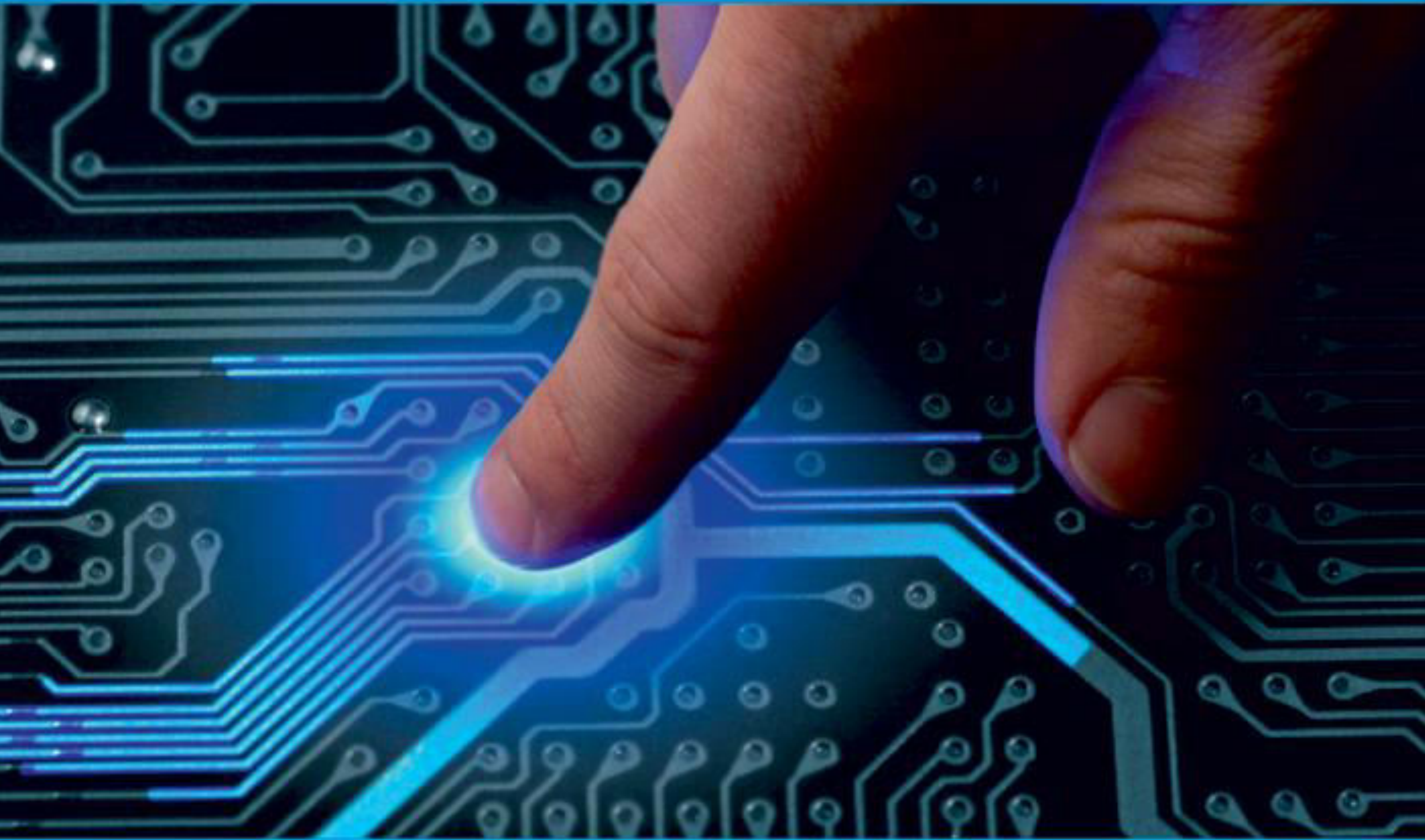
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 9, Septmber 2023

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

| DOI: 10.15680/IJIRCCE.2023.1109025 |

Cybercrimes: The Effect on Public Administration

Dr. Reena Srivastava

Professor in Public Administration, Govt. College, Sirohi, Rajasthan, India

ABSTRACT: In today's period of online processing, most of the information and data is online and thus susceptible to cyber threats. Researchers and crime scholars argue that conflicts and wars between countries will occur in cyberspace as opposed to physical spaces in the future. The first documented cybercrime occurred in the early-19th century. Current computers have come a long way, with neural computing alleging to transform every element in a glass of water into a computer with the ability to conduct innumerable activities in a second. Cybercrime has gained popularity thanks to the increasing reliance on computers in today's life. This paper discusses and analyzes the aspect of cybercrime, including the strategies and impacts of cybercrimes and their types extensively.

KEYWORDS- cybercrimes, public, administration, computers, nations

I.INTRODUCTION

Cyber crime has been increasing in complexity and financial costs since corporations started to utilize computers in the course of doing business. As technology increases between governments that are involved in international business, criminals have realized that this is a cost effective method to make money. This investigation and trial manual is meant to serve as a basic template on the lessons learned to prepare governments, and their prosecutors, for combating cyber crime. To delve deeply into computer technology requires both long study and technical expertise. Therefore, as in most crimes that are technical in nature, or have technical aspects to them, such as bank fraud, murder investigations that require the analysis of blood and spatter techniques, gun-shots that require extensive ballistics investigation, experts are advisable for use as an aid in directing your investigations, to act as a special aide in preparing for trial, and as an expert to testify in that trial. However, experts are not absolutely required, particularly in identifying basic components that make up a cyber crime, and on how to prove the elements of that case. We all know that computer crimes can run from the simple to the ultra sophisticated. [1,2,3] This does not mean they are not solvable, and explainable to the judiciary during any trial. The complexity in these crimes should not be feared. All that is required is for you to understand the basic concepts explained in this manual, follow its simple rules and use that knowledge you have acquired. You will then be able to adequately investigate, prepare and put on any case. External Cyber Attacks External cyber attacks are increasing in frequency and causing extensive damage to companies and organizations. Cyber criminals have also organized into criminal groups that will cause damage for the challenge, pay, extortion, blackmail, etc. External attacks are typically launched from the Internet and circumvent the poor security controls of a government or corporation. Internal Cyber Threats The internal cyber threat is the most damaging to an organization due to the insider knowledge that an internal source has of an agency or company. An example of an internal employee who caused grave damage to an organization is of a police officer that used his inside knowledge of his law enforcement organization and its network to steal sensitive information that he then exchanged with a foreign power for money.

Malicious Software Viruses: Software that attaches itself to a normal file and then reproduces itself to cause damage to a computer system or network. Worms: Software that looks for vulnerabilities in a computer system or network and then reproduces itself.

Trojan horse: This is a program that appears to be a normal program but in reality is used to introduce a malicious program to a computer system or network. Backdoors: Programs that are placed by cyber criminals to gain access to a computer system or network at a later date and time. Viruses This malicious software can be transported by a variety of mechanisms like email. The best protection against viruses is to ensure that all systems have the latest antivirus software. E-Commerce Fraud Criminals use the Internet and computer to defraud victims by posting items that do not exist or are damaged. E-Commerce Fraud is growing at an increasing rate due to the availability and use of the Internet to conduct commerce. Phishing/Identity Theft Phishing involves the use of email or web pages to convince victims to reveal their personal or financial information. The stolen information is then used for the criminal's benefit. Web Hacking Cyber criminals use web hacking to deface government or corporate web sites. This activity is conducted to embarrass and show that the agency or company has weak security.[4,5,6] Hacktivism Hacktivism involves the use of computers and the Internet to conduct resistance against a government or corporation. Hacktivists will conduct Denial of Service (DoS) attacks, intrusions, and web defacing to make a point about their political views. Cyber Espionage Cyber Espionage involves the utilization of computer systems to aid in the act of stealing sensitive information. Cyber Espionage is generally sponsored by a State or a corporation that is attempting to gain an advantage over a competing/adversarial corporation, espionage group or target state or their agencies. Financial Impact of Cyber Crime The overall monetary impact of cyber crime on society and government are unknown. Some estimates are that viruses and worms cause damages into the billions of dollars a year. It is estimated that only 5 - 10% of cyber crime is reported to law enforcement authorities. Reasons why cyber crime is not reported varies from not knowing that a cyber incident has occurred to not wanting the public to know that a company's security data may have been exposed. Cyber Crime Unit Requirements The impact of cyber crime has been, and will be in the future, felt by all governments and economies that are connected to the Internet. Criminals will use the Internet, computers and other digital devices to facilitate their illegal activities. Prosecutors and police must have resources, training and equipment required to address cyber crime in order to keep current on this newest method of crime fighting.

II.DISCUSSION

Cybercrime is a growing threat to individuals in the digital age. With the increasing sophistication of cyberattacks, individuals are becoming more vulnerable to financial loss, identity theft, emotional trauma, and damage to their reputations.

1] On Individuals

- Financial loss or loss of income : One of the most common effects of cybercrime on individuals is financial loss. Cybercriminals often use various methods such as phishing, hacking, and malware to gain access to an individual's financial information, such as credit card numbers, bank account details, and passwords. This can result in the loss of money through unauthorized transactions, which can be difficult to recover.

- Identity theft: Identity theft is another significant consequence of cybercrime for individuals. Cybercriminals can use stolen personal information such as social security numbers, driver's license numbers, and dates of birth to open new accounts, take out loans, and commit other types of fraud in an individual's name. This can result in financial loss and significant legal and administrative headaches in recovering the individual's identity.[7,8,9]

- Emotional trauma: In addition to financial loss and identity theft, cybercrime can cause emotional trauma. Victims of cybercrime often feel violated and vulnerable, leading to fear and anxiety. This can have a long-lasting impact on an individual's mental health, especially if they feel isolated and unable to seek help.

- Loss of reputation: Lastly, cybercrime can cause damage to an individual's reputation. Cybercriminals can use stolen information to post embarrassing or damaging content online, leading to a loss of credibility and trust. The effects of reputational damage can be especially damaging in professional settings, leading to job loss or difficulty finding employment.

2] On Businesses

- Financial loss: Cybercrime can have devastating financial consequences for businesses, particularly small and medium-sized enterprises. A successful cyberattack can result in the loss of funds, intellectual property, and customer data, which can be costly to recover. In some cases, businesses may even be forced to shut down due to the financial impact of cybercrime.

- Damage to reputation: Cybercrime can cause irreparable damage to a business's reputation. A successful cyberattack can expose sensitive customer data, undermining trust and confidence in a business's ability to protect its customers' information. This can lead to losing loyal customers, decreasing revenue, and reducing market share.

- Legal repercussions: Businesses can face significant legal repercussions as a result of cybercrime. Data breaches can result in legal action, fines, and penalties, particularly in heavily regulated industries like healthcare and finance.

- Loss of intellectual property: Cybercriminals can target businesses to steal intellectual property, such as trade secrets and patents. The loss of intellectual property can be a significant blow to businesses, particularly those that rely on innovation and research to remain competitive. It can further lead to decreased revenues, lost opportunities, and reduced market share, potentially affecting the long-term sustainability of the business.

3] On Society

- Economic impact: Cybercrime can have a significant impact on the economy. It can result in financial losses for individuals, businesses, and governments. The cost of repairing damage to systems, recovering lost data, and preventing future attacks can be substantial. It can also impact consumer confidence in online transactions, decreasing business sales and revenue. Additionally, cybercrime can result in the loss of intellectual property, negatively affecting industry innovation and competitiveness.

- National security concerns: Cybercrime can pose a serious threat to national security. Attacks on government and military networks can compromise sensitive information and disrupt operations. Cybercriminals can also use technology to engage in espionage, stealing state secrets, and disrupt critical infrastructure, such as power grids and transportation systems. Additionally, cybercrime can be used for political and ideological purposes, leading to social and political unrest.

- Impact on healthcare and public safety: Cybercrime can have a significant impact on healthcare and public safety. Attacks on healthcare systems can compromise sensitive patient data and disrupt medical services, which can have life-threatening consequences. Additionally, attacks on critical infrastructure, such as emergency response systems and transportation networks, can put public safety at risk. Cybercriminals can also use technology to commit identity theft, which can financially harm individuals.[10,11,12]

- Increase in cyberbullying and harassment: Cybercrime can lead to an increase in cyberbullying and harassment. Cybercriminals can use technology to target individuals and groups, spreading malicious content and harassing messages. This can result in emotional and psychological harm and damage to reputations and relationships. Cyberbullying and harassment can also hurt mental health, leading to depression and anxiety. Additionally, cybercrime can spread misinformation, which can have serious social and political consequences.

- Social media manipulation : A social media manipulation is a form of cybercrime involving using social media platforms to influence, deceive, or manipulate individuals or groups for political, financial, or personal gain. This can take many forms, including spreading false information, creating fake profiles or personas, and using bots or automated accounts to amplify messages.

The effect of social media manipulation on society can be significant, as it can undermine the integrity of democratic processes, promote extremist ideologies, and erode public trust in institutions and information sources.

Hence knowing prevention strategies is important.

Prevention and Mitigation Strategies

Prevention and mitigation strategies are essential in protecting individuals, businesses, and society from the negative impacts of cybercrime. Cybersecurity threats are becoming increasingly sophisticated and prevalent. There are various measures that individuals, businesses, and governments can take to prevent and mitigate the impact of cybercrime, as follows:

1] Cybersecurity measures for individuals:

Individuals can take several measures to ensure protection from cybercrime, including:

- Create strong passwords and use two-factor authentication
- Keeping software and operating systems up-to-date with the latest security patches
- Avoid using public Wi-Fi networks and a Virtual Private Network (VPN)
- Being cautious of suspicious emails and messages, especially those containing links or attachments
- Backing up important data regularly
- Educating themselves about cybersecurity threats and best practices

2] Cybersecurity measures for businesses:

Businesses can take several measures to ensure protection from cybercrime, including:

- Conducting regular security risk assessments
- Implementing access controls and monitoring for suspicious activity
- Providing cybersecurity training for employees
- Implementing strong passwords, two-factor authentication, and encryption for sensitive data
- Implementing a robust backup and disaster recovery plan
- Regularly updating software and hardware systems[13,14,15]

3] Government initiatives and policies:

Governments can implement initiatives and policies to protect citizens from cybercrime, including:

- Establishing cybersecurity standards and regulations for businesses and organizations
- Providing resources and training for individuals and businesses on cybersecurity best practices
- Investing in research and development of new cybersecurity technologies and tools
- Enforcing penalties for cybercrime and holding perpetrators accountable

- Sharing threat intelligence and collaborating with international partners to combat cybercrime globally.

4] Investing in creator insurance:

Investing in creator insurance can provide content creators with financial protection and peace of mind. The top benefits are:

- Creator insurance protects content creators from financial loss due to legal disputes or other risks.
- It covers legal fees, damages, and other costs associated with legal claims, such as copyright infringement, defamation, or privacy violations.
- Creator insurance can also protect intellectual property and cover injuries or damage to property or equipment.
- It provides peace of mind and allows creators to focus on their work without worrying about potential financial losses or legal disputes.

Cybercrime is a growing threat that poses significant risks to individuals, businesses, and society. As technology advances, the number and severity of Cybercrime incidents are expected to increase, leading to devastating financial and reputational losses. We must take action to combat Cybercrime through increased awareness and preventative measures.
Individuals should implement cybersecurity best practices and invest in Cyber insurance. Businesses must prioritize cybersecurity and training to prevent Cybercrime. Governments can implement policies that hold perpetrators accountable and promote cybersecurity best practices.
In short, combating Cybercrime requires a collective effort from individuals, businesses, and governments. By working together and taking proactive steps, we can reduce the risks of Cybercrime and protect ourselves from its devastating consequences.[16]

III.RESULTS

Thanks to digitalization, our phones are not the only assets that have become smart. Artificial intelligence (AI) and the internet of things (IoT) have enabled smart homes, where you can turn on any device with a voice command. Your new–age smart TV allows you to subscribe to various streaming platforms but leaves your payment details susceptible to hacking in the absence of a legitimate security system.

Importance of Cyber Insurance
Damages caused by cybercrimes often transcend financial losses. Data breaches, ransomware, malware, etc., can bring even the largest corporations down to their knees. The impact of cybercrimes on society in general and businesses in particular can be tremendously taxing. However, cybercrime victims can recover their financial losses with cyber insurance.

Cyber insurance covers several cybercrimes, including phishing, ransomware, identity theft social media bullying, online scams, etc. The insurer covers the legal costs, costs associated with repairing devices affected by malware, relocation costs, etc., up to a specific sum insured per the policy terms. Whether you run a business or own a personal computer, you must secure your online presence with cyber insurance.

Cybercrime has become a major concern for public administration as it poses significant threats to the functioning of government institutions. The effect of cybercrime on public administration includes compromised data security, financial loss, disruption of services, and unequal access to information. One of the key impacts of cybercrime is the compromised security of government data. Hackers are able to gain unauthorized access to sensitive information, such as personal, financial, and classified data, putting individuals and institutions at risk. This breach of security can lead to identity theft, financial fraud, and other forms of criminal activities. Financial loss is another significant consequence of cybercrime for public administration. The cost of recovering from cyber-attacks, implementing security measures, and compensating affected parties can be substantial.

Furthermore, financial resources that could be allocated for public service delivery may need to be redirected towards addressing cyber threats, diminishing the overall efficiency and effectiveness of public administration. Cybercrime also disrupts the provision of public services, as government agencies may become incapacitated due to hacking, malware attacks, or ransomware incidents. This can hinder the delivery of essential services, such as healthcare, emergency response, and public transportation, potentially endangering the well-being of citizens. Additionally, cybercrime exacerbates existing inequalities in access to information. Low-income individuals and marginalized communities are often more vulnerable to cyber-attacks due to limited access to reliable and secure technologies. As public administration increasingly relies on digital platforms for information dissemination, those without adequate resources may be left behind, widening the digital divide. To mitigate the effect of cybercrime on public administration, proactive measures are necessary. This includes robust cybersecurity infrastructure, continuous monitoring and assessment of potential risks, training and awareness programs for government employees, and collaboration with cybersecurity experts and agencies. Implementing multi-layered security systems, encryption techniques, and regular data backups can help safeguard government data and protect public administration from cyber threats. Overall, cybercrime has far-reaching consequences on public administration, undermining the security, financial stability, service delivery, and equal access to information. Addressing these challenges requires prioritizing cybersecurity in governance and adopting comprehensive strategies to prevent and respond to cyber threats.[17,18,19]

IV.CONCLUSION

“Cybercrime,” or, in other words, “computer crime,” implies premeditated offenses, atrocities, and illegal actions in the field of computer information. It is a common name for all types of criminal activity committed using computers or the Internet. Cybercrime can be committed using various methods and tools, such as phishing, viruses, spyware, ransomware, and social engineering – most often to steal personal data or financial resources. Moreover, this type of “violation of the rules of society” is equated with terrorism and attacks by various illegal structures and groups. Cybercriminals use the Internet’s interconnection, secrecy, and anonymity, breaking the very foundation of the modern information society. Computer infections, botnets, cyberbullying, cyber pornography, cyber terrorism, identity theft, and cyberstalking are all examples of cybercrime. Today, similar incidents occur in almost all government and public sectors and the daily lives of individuals. Such moments violate stability and the usual way of life. As a result, cybersecurity issues are reaching a new level every year for diplomatic agencies and particular states’ leaders.[20]

REFERENCES

1. Sukhai, Nataliya B. (8 October 2004). "Hacking and cybercrime". Proceedings of the 1st annual conference on Information security curriculum development. New York, NY, USA: ACM. pp. 128–132. doi:10.1145/1059524.1059553. ISBN 1-59593-048-5. S2CID 46562809.
2. ^ Sukhai, Nataliya B. (8 October 2004). "Hacking and cybercrime". Proceedings of the 1st annual conference on Information security curriculum development. New York, NY, USA: ACM. pp. 128–132. doi:10.1145/1059524.1059553. ISBN 1-59593-048-5. S2CID 46562809.
3. ^ "BUFFETT: This is 'the number one problem with mankind'". Business Insider. Retrieved 17 May 2021.
4. ^ "Warren Buffett: 'Cyber poses real risks to humanity'". finance.yahoo.com. 30 April 2019. Retrieved 17 May 2021.
5. ^ "The Global Risk Report 2020" (PDF). World Economic Forum. 15th Edition: 102. 15 January 2020.
6. ^ Heading, Sophie; Zahidi, Saadia (January 2022). "The Global Risks Report 2022, 18th Edition" (PDF). World Economic Forum.
7. ^ a b Freeze, Di (12 October 2022). "Cybercrime To Cost The World $9.5 trillion USD annually in 2022". Cybercrime Magazine. Retrieved 3 February 2022.
8. ^ Gordon, Sarah (25 July 2006). "On the definition and classification of cybercrime". Journal in Computer Virology. 2: 13–20. doi:10.1007/s11416-006-0015-z. S2CID 3334277.
9. ^ a b Richet, Jean-Loup (1 January 2022). "How cybercriminal communities grow and change: An investigation of ad-fraud communities". Technological Forecasting and Social Change. 174 (121282): 121282. doi:10.1016/j.techfore.2021.121282. ISSN 0040-1625. S2CID 239962449.
10. ^ Lehman, Jeffrey; Phelps, Shirelle (2005). West's Encyclopedia of American Law, Vol. 3 (2 ed.). Detroit: Thomson/Gale. p. 137. ISBN 9780787663742.

11. ^ "Computer and Internet Fraud". LII / Legal Information Institute. Retrieved 1 November 2020.
12. ^ Parker D (1983) Fighting Computer Crime, U.S.: Charles Scribner's Sons.
13. ^ "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress". www.everycrsreport.com. Retrieved 5 September 2021.
14. ^ Lepofsky, Ron. "Cyberextortion by Denial-of-Service Attack" (PDF). Archived from the original (PDF) on 6 July 2011.
15. ^ Mohanta, Abhijit (6 December 2014). "Latest Sony Pictures Breach : A Deadly Cyber Extortion". Archived from the original on 25 September 2015. Retrieved 20 September 2015.
16. ^ "The Growing Ransomware Threat: 4 Trends and Insights". Palo Alto Networks. 25 March 2022. Retrieved 11 May 2022.
17. ^ "100+ ransomware statistics for 2022 and beyond - Norton". us.norton.com. Retrieved 11 May 2022.
18. ^ Carback, Joshua T. (2018). "Cybersex Trafficking: Toward a More Effective Prosecutorial Response". Criminal Law Bulletin. 54 (1): 64–183. p. 64.
19. ^ "IJM Seeks to End Cybersex Trafficking of Children and #RestartFreedom this Cyber Monday and Giving Tuesday". PR Newswire. 28 November 2016.
20. ^ ^{a} ^{b} "Cybersex Trafficking". IJM. 2020.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH
IN COMPUTER & COMMUNICATION ENGINEERING