International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 10-01-2024, Accepted: 25-01-2024, Published: 09-02-2024
Volume 6, Issue 1, 2024, Page No. 73-77

Cyber security necessity and benefits

Aditya Tiwari[1], Shivangi Sinha[2]
[1] Department of Law, Bharati Vidhyapeeth University Pune, Maharashtra, India
[2] Assistant Professor, Department of Law, Bharati Vidhyapeeth University Pune, Maharashtra, India

Abstract
In the digital era, cybersecurity stands as an indispensable pillar for safeguarding information systems, networks, and data from malicious threats. This research paper delves into the imperative need and multifaceted benefits of robust cybersecurity measures in our increasingly interconnected world.
The paper commences by elucidating the escalating cyber threats prevalent in diverse sectors, emphasizing the criticality of proactive cybersecurity measures. It explores the evolving landscape of cyber threats, encompassing malware, phishing attacks, ransomware, and other sophisticated intrusions that pose substantial risks to individuals, organizations, and nations.
Furthermore, the research emphasizes the crucial role of cybersecurity in preserving confidentiality, integrity, and availability of sensitive information. It outlines the significance of implementing robust security protocols, encryption techniques, and access controls to fortify digital infrastructures against potential breaches.
The study also examines the multifaceted benefits of cybersecurity implementation, encompassing not only risk mitigation but also fostering trust and reliability among stakeholders. It highlights the role of cybersecurity in bolstering consumer confidence, ensuring business continuity, and complying with regulatory standards.
In this paper highlights that cybersecurity is not merely an option but an absolute necessity in today's digital landscape. By understanding the risks, implementing proactive measures, and recognizing the manifold benefits, individuals, organizations, and governments can fortify their defenses and navigate the complexities of the cyber realm with confidence and resilience.

Keywords: Technology, Cyber, organizational, criminal

Introduction

Cyberattacks happen frequently; as we speak, the security of certain organizations, no matter how big or little, is at risk. For instance, we may observe all the current cyberattacks if you go to the "threat cloud" website. It provides the scope of real-world cyberattacks that occur on a regular basis. These days, a lot of our daily tasks include the internet. However due to this digital interconnectedness has also opened the door to an array of cyber threats, ranging from malicious software and phishing attacks to sophisticated hacking endeavors. In response to these challenges, the field of cybersecurity has emerged as a critical line of defense, aiming to protect digital systems, networks, and data from unauthorized access, exploitation, and compromise but we must continue to be aware of the system and the notifications we get. The manner cybercriminals commit crimes is also evolving daily due to the advancements in information technology.

There are several obstacles in the way of enforcing cybercrime laws in any community as the criminal scenario in cyberspace differs greatly from that of physical space. In contrary to the internet, where age is not as self-authenticating, age is a self-authenticating component in physical space. In cyberspace, a minor under the age of eighteen can readily pass for an adult and gain access to resources that are limited, something that would be challenging for him to achieve in physical space. Cybersecurity is defending data by averting, identifying, and countering online threats.

As our dependence on digital technologies deepens, the importance of cybersecurity cannot be overstated. Beyond protecting sensitive information, cybersecurity is integral to maintaining public trust, ensuring business continuity, and safeguarding national security interests. Organizations and individuals alike must recognize cybersecurity as an essential component of responsible digital citizenship.

Objective of the Study

1- Assessment of Cyber Threat
2- Effectiveness of Cybersecurity Measures
3- Impact on Data Protection and Privacy

Research Questions

1. To what extent do prevailing cyber threats pose risks to the confidentiality, integrity, and availability of digital assets, and how does the necessity of cybersecurity measures evolve in response to these threats?
2. What is the impact of effective cybersecurity measures on organizational resilience, business continuity, and financial outcomes, and how does this contribute to quantifiable benefits such as cost savings and reputation enhancement?
3. How do user awareness and education initiatives influence the successful implementation of cybersecurity measures, and what role does user behavior play in determining the overall effectiveness of cybersecurity strategies?

Definition

There is no universally accepted definition of cybercrime. However, the following. (1) [1] definition includes elements common to existing cybercrime definitions. Cybercrime is an act that violates the law, which is perpetrated using information and communication technology (ICT) to either target networks, systems, data, websites and/or technology or facilitate a crime.

Cybercrime is defined as "criminal activities carried out through the utilization of computers, computer networks, and digital technologies, encompassing a spectrum of illicit actions that exploit vulnerabilities in digital systems, with the intent of financial gain, unauthorized access, disruption, or malicious activities".

Example

1. Stealing credit card information.
2. Breaking into the government website
3. Email and Internet fraud.
4. Identity fraud.
5. Theft and sale of corporate data.
6. Ransomware attacks.
7. Cyberextortion (demanding money to prevent a threatened attack).
8. Cyber Spying (where hackers access government or company data).

History

It's hard to pinpoint the precise moment when a crime was committed via a computer network, or the morning of cybercrime.

The first case of use of computer theft was in 1973, A teller at a original New- York bank used a computer to embezzle over 2 million. The first spam dispatch took place in 1978. transferring spam emails is a cybercrime.

In certain countries, we can be behind bars if we shoot spam emails. In the 1980's MNC Database (pentagon and IDM) was addressed.

The first VIRUS was installed on Apple computers in 1982.

In 2016, Kaspersky: one of the leading antivirus providers to the world reported around 758 million malicious attacks that occurred.

Types of Cyber Crime

Malware Attacks

Malware, or malicious software, refers to any set purposely intended to cause harm to a computer, server, network, or usage. It includes a variety of harmful programs such as viruses, worms, Trojans, ransomware, and spyware. Malware aims to compromise the confidentiality, integrity, or availability of data and may lead to unauthorized access, data theft, or system disruption. Preventative measures, such as antivirus software and regular system updates, are crucial to defending against malware attacks.

Trojans

A Trojan Horse, or simply a Trojan, is a type of malicious software that disguises itself as legitimate or helpful software. Unlike viruses, Trojans don't replicate but trick users into installing them. Once inside a system, they can perform various harmful actions, such as stealing data, providing unauthorized access, or delivering additional malware. Named after the ancient Greek story of a deceptive wooden horse, Trojans deceive users by appearing harmless while hiding malicious intent. Protective measures, like cautious downloading and robust cybersecurity, are crucial to defend against Trojan attacks

Worms

Worms infect entire networks of devices either locally or across the internet by using the network interfaces. It uses each consecutive infected machine to infect more.

Password Attack

An effort to steal or decode a user's password for illegal activities. Hackers can utilise cracking programmes, dictionary assaults, and password sniffers to conduct password attacks.

Password assaults may be prevented by implementing a password policy that includes minimum length, unrecognisable terms, and regular changes.

Phishing

It's a cybercrime where people are communicated through phone calls, dispatch, or a communication by cybercriminals posing as a person from a legitimate institution. A phishing crusade is when spam emails, or other forms of communication, are transferred to emails, to trick donors into doing commodity that undermines the security or security of the association they work for. These cybercriminals collect particular information like bank account details and watchwords and also steal plutocrat. dispatches transferred by phishing look authentic and attempt to get victims to reveal their information.

Cybercrime and Information Security

- **Firewalls and Security Software** [2]

Use firewalls to monitor and control incoming and outgoing network traffic.

Employ antivirus and anti-malware software to detect and remove malicious programs.

- **Regular Software Updates**

Keep all operating systems, software, and applications up to date with the latest security patches.

Enable automatic updates whenever possible.

- **Strong Authentication**

Implement multi-factor authentication (MFA) to add an extra layer of security beyond usernames and passwords.

- **Employee Training and Awareness**

Conduct regular cybersecurity awareness training for employees to recognize and avoid common threats like phishing.

Emphasize the importance of strong password practices.

- **Access Control**

Restrict access to sensitive data and systems based on the principle of least privilege.

Regularly review and update user permissions.

- **Network Segmentation**

Divide the network into segments to limit the potential impact of a cyber attack. This can help contain and isolate malicious activity.

- **Incident Response Plan** [3]

Develop and regularly update an incident response plan outlining the steps to be taken in the event of a cyber attack.

Conduct drills to ensure a quick and effective response.

- **Data Encryption**

Encrypt sensitive data, both in transit and at rest, to protect it from unauthorized access.

- **Backup and Recovery**

Regularly back up critical data and ensure backups are stored securely.

Test data restoration processes to ensure quick recovery in case of a cyber attack.

- **Phishing Protection**

Use email filtering tools to detect and block phishing attempts.

Train employees to recognize phishing emails and avoid clicking on suspicious links or downloading attachments.

- **Mobile Device Security**

Implement security measures for mobile devices, including strong passcodes, remote wipe capabilities, and mobile device management (MDM) solution

Cybersecurity

Technologies and processes designed to protect networks and devices from attack, damage or unauthorized access.

Advantages

1. Increased productivity
2. Protection for your customers or client
3. Inspires customer confidence.
4. Stops your website from crashing.
5. Protection of our business

Why do we need cyber security?

The Three main Pillars of cyber security are

- **Confidentiality**

(Data should be nonpublic) the principle of confidentiality asserts that the information and functions can be entered only by certified party.

- **Integrity**

(Data Integrity should be complete) the principles of integrity assert that information and functions can be added, altered, or removed only by sanctioned people and means.

- **Availability**

(Data should be available) the principles of availability assert that systems, functions, and data must be available on demand according to agreed- upon parameters grounded on situations of service.

India's cybersecurity law

India has enacted several laws and regulations related to cybersecurity to address the challenges posed by cyber threats.

Information Technology Act, 2000

The Information Technology (IT) Act, 2000 is the primary legislation in India that addresses various aspects of electronic governance and electronic commerce. It contains provisions related to unauthorized access, hacking, data protection, and the punishment for cybercrimes.

Amendments to the IT Act in 2008

The IT Act was amended in 2008 to address emerging cyber threats more comprehensively. The amendments introduced new offenses, including unauthorized interception, identity theft, and the publication of sexually explicit material.

National Cyber Security Policy, 2013
While not a law per se, the National Cyber Security Policy provides a framework for enhancing the security posture of the country in cyberspace. It aims to protect information infrastructure, build capabilities to prevent and respond to cyber threats, and foster a resilient cyberspace ecosystem.

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016
The Aadhaar Act is significant for its role in managing the Aadhaar biometric identity system. It contains provisions related to the security and confidentiality of identity information.

Data Protection Laws and Regulations
India is in the process of formulating a comprehensive data protection law. As of my last update, the Personal Data Protection Bill, 2019, was introduced in the Indian Parliament. The bill aims to regulate the processing of personal data, including data related to cybersecurity.

Indian Penal Code (IPC)
The IPC includes sections that can be applicable to cybercrimes, such as sections dealing with fraud, forgery, and identity theft. When cybercrimes involve traditional offenses, the IPC may be invoked.

Banking Regulations
The Reserve Bank of India (RBI) issues guidelines and regulations to ensure the cybersecurity of banks and financial institutions. These guidelines focus on securing online transactions, customer data protection, and incident reporting.

Emerging Trends in Cybersecurity
Cybersecurity is dynamic and constantly evolving to address new threats and challenges. Here are some emerging trends in cybersecurity that are relevant:
Artificial Intelligence in Cybersecurity [4]
Using AI and ML to enhance threat detection and response capabilities.
Predictive analytics for identifying and preventing potential security incidents.

Zero Trust Architecture
Moving away from traditional perimeter-based security models to a model that assumes no trust, even within the network.
Continuous authentication and authorization are crucial components.

Cloud Security
Addressing security challenges associated with cloud adoption.
Implementing robust cloud security strategies and tools.

IoT Security
Securing the growing number of connected devices on the Internet of Things.
Managing vulnerabilities in IoT devices and networks.

Blockchain Technology
Exploring the use of blockchain for enhancing security and transparency in various applications.
Secure and decentralized authentication and authorization mechanisms

Ransomware Defense Strategies
Developing and executing efficient defense techniques against ransomware attacks. Improving incident reaction and recovery plans.

Biometric Authentication
Increasing the usage of biometrics for user authentication. Addressing confidentiality and safety concerns about biometric data.

Challenges and Future Directions in Cyber Security
Challenges
Complex Cyber Threats [5]
Cyber dangers are becoming increasingly complex, including advanced persistent threats (APTs) and state-sponsored assaults.

Rapidly Evolving Technology
observing up with the rapid-fire pace of technological advancements, similar as IoT, 5G, and AI, which introduce new vulnerabilities.

Insider hazards
Dealing with insider threats, purposeful or unintentional, from workers or individuals with access to sensitive information.

Supply Chain Vulnerabilities
Challenges relating to and securing supply chain vulnerabilities to prevent attacks similar as software supply chain negotiations.

Deficit in Cybersecurity Skills
A global shortage of professed cybersecurity professionals, making it challenging for associations to make and keep up effective security teams.

Outdated Software [6]
If you don't keep your apps and software updated, they can be exploited and hacked with ransomware, or as we've seen from the Bluekeep attacks in 2019, your unpatched software can be exploited to install cryptocurrency miner

Future Directions
Quantum-Safe Cryptography [7]
Creation and implementation of cryptography methods that can withstand assaults from quantum computers.

AI-Driven Security
Increased usage of artificial intelligence and machine learning for proactive threat identification and response.

Zero Trust Architecture
Broad adoption of a trustless security model where trust is never expected, and continuous authentication is implemented.

Blockchain for Security [8]
Exploring the use of blockchain technology to improve security, particularly in areas such as identity management and secure transactions.

Automation and Orchestration
Increasing automation of information security processes and orchestrating incident response for greater efficiency.
International Cooperation
Strengthen international cooperation on cyber security standards and information sharing against global threats.

User-Centric Security
Designing security measures with a focus on user experience to encourage better adoption of security practices.

Case Law
Notable cybersecurity Incidents
Bharat Interface for Money (BHIM) App Data Leak (2020) The BHIM app, a government- supported digital payments operation, faced a data leak in 2020. information of millions of users was allegedly available for trade on the dark web.
Wipro Data Breach (2019) IT services company Wipro felt a data breach in 2019 [9]. bushwhackers reportedly used phishing emails to compromise hand accounts and launch attacks on Wipro's customers.
UIDAI Data Breach (2018) There were reports of contended Aadhaar data breaches, the unique identification number issued by the Unique Identification Authority of India (UIDAI). The authority denied any breach, but enterprises were raised about the security of the Aadhaar system.
Ransomware Attacks on Kerala Government Websites (2017) Several government websites in the state of Kerala were targeted by ransomware in 2017. The attackers demanded a ransom in bitcoin to restore access to the affected websites.
Indian Railways E-ticketing Portal Hacked (2016) [10]
The Indian Railways' online ticketing portal faced a cyber-attack in 2016, affecting the booking and payment systems. The website was temporarily taken down for security measures.
Cosmos Bank Cyber Attack in Pune A cyber-attack in India in 2018 was deployed on Cosmos Bank in Pune. This daring attack shook the whole banking sector of India when hackers siphoned off Rs. 94.42 crores from Cosmos Cooperative Bank Ltd. in Pune.

Recommendation
Certainly, exploring future research topics in cybersecurity is crucial as the field continues to evolve. Here are some recommendations for research topics focusing on the necessity and benefits of cybersecurity:

Human-Centric Cybersecurity
Examine how human behaviour affects cybersecurity, with a focus on user awareness, education, and how human factors affect the security posture

Cybersecurity for Emerging Technologies
Examine the advantages and need for cybersecurity precautions for cutting-edge technology including artificial intelligence, quantum computing, and the Internet of Things (IoT).

Cybersecurity Awareness Program
Examine how well cybersecurity awareness programmes work in various settings and investigate how learning efforts can create a safer online world.

Privacy-Preserving Technologies
Examine cutting-edge tools and techniques that protect user privacy while guaranteeing cybersecurity, particularly considering the rise in data collecting and analysis.
Discover the role of AI in improving threat intelligence capabilities and explore how AI-powered analytics can improve the speed and accuracy of cyber threat detection and mitigation.

Legal and Regulatory Impact on Cybersecurity
Explore the impact of current and evolving legal and regulatory frameworks on cybersecurity and explore how compliance can contribute to an organization's security and overall cyber resilience.

Conclusion
Cyber security is a broad issue that is growing increasingly vital as the world becomes more linked, with networks utilized to carry out critical activities. With each New Year, cybercrime diverges into new directions, as does information security. The most recent and disruptive technologies, as well as new cyber tools and attacks that emerge daily, are presenting organizations with new challenges in not just securing their infrastructure, but also requiring new platforms and intelligence to do so. There is no perfect answer to cybercrime, but we should do our utmost to minimize it to have a safe and secure future in cyberspace.

References
1. https://www.unodc.org/e4j/en/cybercrime/module
2. https://shardsecure.com/blog/enterprise-data-security-guide
3. https://logmeonce.com/resources/security-of-network-services/
4. https://www.forbes.com/sites/bernardmarr/2023/10/11/the-10-biggest-cyber-security-trends-in-2024-everyone-must-be-ready-for-now/?sh=255192395f13
5. https://www.aztechit.co.uk/blog/cyber-security-issues-challenges-for-businesses
6. https://www.scmagazine.com/home/security-news/cybercrime/attackers-attempt-large-scale-bluekeep-exploit-to-spread-cryptominer/
7. https://www.bmc.com/blogs/it-orchestration-vs-automation-wha....
8. https://www.simplilearn.com/top-cybersecurity-trends-article
9. https://www.thehindu.com/sci-tech/technology/major-cybersecurity-data-breaches-in-2023/article67644589.ece
10. https://kratikal.com/blog/5-biggest-cyber-attacks-in-india/