IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

CYBER SECURITY INSIGHTS

[1]Bhagyashree **[2]Sridevi B** **[3]Srinivas R**

[1]Assistant Professor [2]Assistant Professor [3]Assistant Professor

[1]Department of Computer Applications, Vishwa Chethana Degree College, Anekal, Bangalore, Karnataka

[2]Department of Computer Applications, Vishwa Chethana Degree College, Anekal, Bangalore, Karnataka

[3]Department of Computer Applications, Vishwa Chethana Degree College, Anekal, Bangalore, Karnataka

Keywords: Authentication, Vulnerability, Cyber Threat Intelligence, Encryption, Firewall, Malware, Endpoint Security, critical infrastructure.

Abstract: Use of the term "cyber security" as a key challenge and a synonym for information security or IT security confuses customers and security practitioners, and obscures critical differences between these disciplines. Within this paper, we are aiming to explain "cyber security" and describe the relationships among cyber security, information security, OT security, IT security, and other related disciplines and practices, e.g. cyber defence, related to their implementation aligned with the planned or existing cyber security strategy at the national level. Cyber security is essential because military, government, financial, medical and corporate organizations accumulate, practise, and stock unprecedented quantities of data on PCs and other devices. Cyber security consists of the infrastructure required to secure the data communicated across the grid, including protection against malicious attacks. The roadmap for cyber security addresses the evaluation and implementation of secure and standard protocols where applicable

Introduction: Cyber security is the way of secure systems, networks, and programs from digital attacks. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes. Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known

as information technology security or electronic information security. Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber attacks. It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks, and technologies. "Cyber Security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access."

"Cyber Security is the set of principles and practices designed to protect our computing resources and online information against threats."

The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cyber security. We can divide cyber security into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called electronic information security or information technology security.

Research methodology:

The present study is conceptual and purely based on the secondary data which is collected from book, journal, published reports and other websites.

Objectives:

1. To study and examine the Effect of cyber security on Encryption.
2. To study and examine the Effect of cyber security on Access control
3. To study and examine the Effect of cyber security on Vulnerability.
4. To study and examine the Effect of cyber security on Authentication.
5. To study and examine the Effect of cyber security on Authorization.
6. To study and examine the Effect of cyber security on Physical security.
7. To study and examine the Effect of cyber security on confidentiality.
8. To study and examine the Effect of cyber security on Integrity.

1. To study and examine the Effect of cyber security on Encryption.

Encryption is a form of data security in which information is converted to cipher text. Only authorized people who have the key can decipher the code and access the original plaintext information. Encryption is a logical process, whereby the party receiving the encrypted data—but also in possession of the key—can simply decrypt the data and turn it back into plaintext. The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted over the internet or other computer networks. It is used to safeguard a wide range of data, from PII to sensitive corporate assets to government and military secrets.

2. **To study and examine the Effect of cyber security on Access control**

Access control is a process that allows companies to determine who has access to sensitive applications and data**.** Access control systems check the identity of users and assign access rights according to user roles. They exclude illegitimate users, reducing the risk of data breaches and other cyber-attacks. Access control prevents data breaches and excludes malicious attackers. The primary goal is to minimize security risks by ensuring only authorized users, systems, or services have access to the resources they need. It involves identifying an individual or system, authenticating their identity, authorizing them to access the resource, and auditing their access patterns. This process minimizes the risk of unauthorized access, protecting sensitive information and systems.

3. **To study and examine the Effect of cyber security on Vulnerability.**

The goal of this study is to identify and analyze the common cyber security vulnerabilities. Vulnerability in security refers to a weakness or opportunity in an information system that cybercriminals can exploit and gain unauthorized access to a computer system. Vulnerabilities weaken systems and open the door to malicious attacks. Common cyber security vulnerabilities that cybercriminals can exploit include weak credentials, lack of data encryption, misconfigurations, out-of-date software and zero days. These vulnerabilities often lead to cyber attacks that bypass an organization's security measures and steal confidential data. A vulnerability scanner can automatically identify many of the vulnerabilities in an organization's systems. Performing a vulnerability scan provides insight into the issues that need correction and where the company is most likely to be attacked.

4. **To study and examine the Effect of cyber security on Authentication.**

Authentication is the process of verifying a user or device before allowing access to a system or resources. Authentication is the process that companies use to confirm that only the right people, services, and apps with the right permissions can get organizational resources. It involves a process of ensuring that the user claiming to be a specific personality is substantial through proving credentials like passwords, biometric data, security tokens, or other authenticity factor. Authentication prevents unauthorized users from accessing networks, websites, databases, and other resources. This helps to prevent data breaches and cyber attack.

5. **To study and examine the Effect of cyber security on Authorization.**

Authorization is the process of giving a user permission to access information or a physical location. Authorization is an important cyber security process that controls access to sensitive data and resources, and prevents unauthorized access Authorization is an important measure in computer security, as it helps to protect information and systems from unauthorised access. The function of authorization is to specify what access rights a user or program has to system resources. This can include files, directories, network resources, and other system objects

6. **To study and examine the Effect of cyber security on Physical security.**

Physical security aims to protect people, property, and physical assets from any action or event that could lead to loss or damage. Physical security is crucial, and security teams must work together to ensure the security of digital assets. physical security protects against unauthorized access (Protect), detects breaches through surveillance and access controls (Detect), and provides a human response to incidents (Respond).

7. **To study and examine the Effect of cyber security on confidentiality.**

Data confidentiality refers to the practice of safeguarding information from unauthorised access, disclosure, or alteration. In essence, it ensures that only those with the appropriate permissions can access sensitive data, shielding it from prying eyes and potential misuse. It provides Protecting Privacy and Reputation, Minimising Attack

Surfaces, Enabling Secure Operations, Compliance with Regulations, Building Trust and Confidence in organizations.

8. **To study and examine the Effect of cyber security on Integrity**

Integrity refers data is complete, trustworthy and has not been modified or accidentally altered by an unauthorised user. The integrity of data can be compromised unintentionally by errors in entering data, a system malfunction, or forgetting to maintain an up-to-date backup.

It processes that ensures the accuracy, completeness, consistency, and validity of an organization's data. it plays a major role in ensuring accountability and transparency within the organization.

Literature review:

A cyber security control V&V process model is built in this study to solve the problem, based on the principle of adaptive focusing testing. Additionally a quantitative approach is built to define and prioritize fault-prone information security controls. It has been verified that the model built may provide an additional and more reliable framework for expert subjective judgment. The aim of this paper is to research the idea of a cyber range, and to include a comprehensive analysis of literature covering unclassified cyber ranges and safety test beds. he review also identifies future research opportunities in emerging cyber security application areas, advanced AI methods, data representation, and the development of new infrastructures for the successful adoption of AI-based cyber security in today's era of digital transformation and polycrisis. Therefore, our objective was to provide a systematic review, a comprehensive view of AI use cases in cybersecurity, and a discussion of the research challenges related to the adaptation and use of AI for cyber security to serve as a reference for future researchers and practitioners.

Findings:

1. Improvements to the cybersecurity posture of individuals, firms, government agencies, and the nation have considerable value in reducing the loss and damage that may be associated with cyber security breaches.
2. Cyber security provides essential protection for both businesses and individuals.
3. Network Security protects communication paths between computers. Uses firewalls and encryption to secure data travelling across networks.
4. Cloud Security protects data stored online from theft, leakage, and deletion. This is essential as more businesses and individuals use cloud storage.
5. Endpoint Security Secures devices like computers and smart phones that connect to networks. Acts as a guard for each device.
6. Mobile Security focuses on protecting smart phones and tablets from threats like malicious apps and unsecured Wi-Fi.
7. Data Security protects data throughout its lifecycle using encryption and access controls.
8. Operational Security involves strategies and decisions for handling and protecting data assets. Creates overall plans for data protection.

Suggestions:

- Don’t fall victim to a phishing scam
- Keep software up-to-date

- Avoid opening suspicious emails
- Keep hardware up-to-date
- Use a secure file-sharing solution to encrypt data
- Use a VPN to privatize your connections
- Disable Bluetooth when you don't need it
- Enable 2-Factor Authentication
- Don't store important information in non-secure places
- Scan external storage devices for viruses
- Use HTTPS on your website
- Use Public Wi-Fi safely
- Never reuse passwords
- Clean up your digital past
- Lock down privacy and security settings
- Build a strong password
- Back up your data

Conclusion:

With the rapid advancement of technology, our lives are becoming increasingly digitalized. People now live in a cyber-world where all data and information is stored digitally and online. Whether it's for business, education, shopping, or banking, practically everything is now done online. The focus on cyber security is frequently on attempting to characterize the problem and determine the genuine threat level. All individuals, professionals, legislators, and, more broadly, all decision makers are concerned about cyber security. Cyber security is critical to the advancement of both information technology and Internet services. Cyber-attacks will be on the rise in 2023-24, and not just from the solitary hackers we've come to associate with them, but also from nation-state actors looking to steal data from governments and organizations. Because cyberspace has no borders, a nation's cyberspace is a component of the global cyberspace and cannot be isolated to define its bounds. It has never been easy to maintain cyber security. And, because assaults are becoming more innovative every day, it's vital to define cyber security and determine what constitutes excellent cyber security. Cyber security is a technology that was designed to protect data and information systems kept on computers. This paper comprehensive review covers cyber security, its objectives. The state or process of safeguarding and recovering networks, devices, and programmes from any sort of cyber-attack is known as cyber security.

References:

1. Lillian Ablon, Martin C. Libicki and Andrea A. Golay, Markets for Cybercnme Tools and Stolen Data: Hackers‟ Bazaar, pp. 1-85, 2014
2. Yusuf Perwej, "An Experiential Study of the Big Data", International Transaction of Electrical and Computer Engineers System (ITECES), USA, ISSN (Print): 2373-1273 ISSN (Online): 2373-1281, Science and Education Publishing, Volume 4, No. 1, Pages 14-25, 2017, DOI: 10.12691/iteces-4-1-3

3. Brenner SW. Cybercrime metrics: old wine, new bottles? Va. JL & Tech, 9:13–13, 2004
4. M. Cross and D. L. Shinder, Scene of the cybercrime.Syngress Pub., 2008
5. Edwards B, Hofmeyr S, Forrest S. Hype and heavy tails: a closer look at data breaches. J Cyber security 2016;2:3–14
6. Ying-Yu Lin. “China Cyber Warfare and Cyber Force.” Tamkang Journal of InternationalmAffairs, vol. 22, no. 3, pp. 119–161, 2019.
7. C.M. Williams, R. Chaturvedi and K. Chakravarthy, "Cybersecurity Risks in a Pandemic", Journal of Medical Internet Res., vol. 22, no. 9, pp. 23692, 2020
8. X. Jin, W. Sun, Y. Liang, J. Guo and Z. Xie, "Design and implementation of intranet safety monitoring platform for Power secondary system", Automation of Electric Power System, pp. 99- 104, Aug. 2011
9. F. Pasqualetti, F. Dorfler and F. Bullo, "Attack detection and identification in cyber-physical systems", IEEE Transactions on Automatic Control, vol. 58, no. 11, pp. 2715-2729, 2013
10. Ali, "Ransomware: A research and a personal case study of dealing with this nasty malware", Issues in Informing Science and Information Technology Education, vol. 14, pp. 87-99, 2017
11. R. Sabillon, J. Cano, V. Cavaller and J. Serra, "Cybercrime and Cybercriminals: A Comprehensive Study", International Journal of Computer Networks and Comm. Security, vol. 4, no. 6, pp. 165-176, 2016
12. Bag, S. Ruj and K. Sakurai, "Bitcoin block withholding attack: Analysis and mitigation", IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, pp. 1967-1978, 2017
13. Arjan Jeckmans, Andreas Peter, and Pieter Hartel. “Efficient privacy-enhanced familiarity based recommender system”, In Computer Security–ESORICS 2013, pages 400–417. Springer, 2013.
14. Pranggono and A. Arabo, "COVID-19 pandemic cybersecurity issues", Internet Technology Letter (Wiley), pp. 1-6, 2020