ASSESSING CYBER SECURITY AWARENESS AND PREPAREDNESS: A SURVEY STUDY

Sivaguru R[1],
Malarvizhi P[2],
Saranya R[3],
Babu G[4]
Saranya K[5]

ABSTRACT

The rapid growth of technology and the increasing reliance on digital systems have highlighted the need for effective cyber security measures. This survey study aims to assess the level of cyber security awareness and preparedness among individuals and organizations. By collecting data through a survey questionnaire, this study seeks to identify gaps in knowledge, identify common vulnerabilities, and understand the current practices in place to mitigate cyber threats. The findings of this study will provide insights into the effectiveness of existing cyber security awareness programs and inform strategies for enhancing cyber security education and preparedness.

Keywords— cyber security awareness, cyber security preparedness, survey study, gaps in knowledge, common vulnerabilities, current practices, cyber threats

INTRODUCTION

Background:

In today's interconnected world, cyber security has become a critical concern for individuals, organizations, and governments. With the rapid advancement of technology and the increasing reliance on digital platforms [1], the risk of cyber threats has grown exponentially. Cyber-attacks can result in financial losses, reputational damage, and the compromise of sensitive data. Therefore, it is essential to understand the level of cyber security[2] awareness and preparedness among individuals and organizations to effectively address these risks.

Problem Statement:

Despite the growing awareness of cyber threats, many individuals and organizations still lack the necessary knowledge and practices to protect themselves adequately. This knowledge gap can leave them vulnerable to various cyber-attacks, such as phishing, malware, ransomware, and social engineering[3]. Furthermore, the constantly evolving nature of cyber threats makes it challenging to stay updated with the latest security measures. Therefore, there is a need to assess the level of cyber security awareness and preparedness to identify potential gaps and develop targeted strategies for improvement.

Objectives:

1. The main objectives of this survey study are as follows:
2. To assess the level of cyber security awareness among individuals and organizations.
3. To evaluate the current cyber security practices and measures implemented by individuals and organizations[5].
4. To identify potential gaps and challenges in cyber security awareness and preparedness.
5. To provide recommendations for enhancing cyber security awareness and preparedness.
6. To contribute to the development of effective strategies and initiatives for mitigating cyber threats.

[1,2,3,4,5]*Department of Computer Science and Engineering, Knowledge Institute of Technology, Salem*

Cyber Security Awareness:

Cyber security awareness refers to the level of knowledge and understanding individuals and organizations have about potential cyber threats and the measures they can take to protect themselves [6]. Several studies have emphasized the importance of cyber security awareness in preventing and mitigating cyber-attacks. These studies highlight the need for individuals to be aware of common cyber threats, such as phishing emails, social engineering techniques, and weak passwords. Furthermore, research has shown that cyber security awareness programs can significantly improve individuals' ability to identify and respond to potential threats.

Cyber Security Preparedness:

Cyber security preparedness focuses on the actions taken by individuals and organizations to protect their digital assets and mitigate the impact of cyber-attacks. This includes implementing robust security measures, such as firewalls, antivirus software, and encryption protocols[7]. Effective cyber security preparedness also involves regular system updates, data backups, and incident response plans. Research has indicated that organizations with well-defined cyber security[8] preparedness measures are better equipped to detect, respond to, and recover from cyber-attacks.

Existing Survey Studies:

Several survey studies have been conducted to assess cyber security awareness and preparedness levels among individuals and organizations. These studies have provided valuable insights into the current state of cyber security practices and identified areas for improvement[9]. Some surveys have focused on specific industries or sectors, such as healthcare, finance, or government, while others have targeted the general population. These studies have examined factors such as knowledge of cyber threats, use of security tools and techniques[10], and awareness of best practices. The findings of these surveys have informed the development of targeted awareness campaigns, training programs, and policy recommendations

Methodology

The methodology of cyber security refers to the systematic approach or set of steps followed to ensure the security of computer systems, networks, and data from cyber threats. While different organizations and experts may have variations in their methodologies [11], the following steps are commonly included:

Risk assessment: Identify and assess potential risks and vulnerabilities to the organization's systems, networks, and data. This includes evaluating the likelihood and impact of potential threats, such as malware, unauthorized access, or data breaches.

Security policy development: Establish a comprehensive and documented security policy that outlines the organization's goals[12], objectives, and guidelines for protecting information assets. This policy should align with industry best practices and regulatory requirements.

Security controls implementation: Implement appropriate security controls to mitigate identified risks. This includes technical controls (firewalls, antivirus software, encryption), procedural controls (access control policies, incident response procedures), and physical controls (video surveillance, access card systems).

Security awareness and training: Educate employees and stakeholders about their roles and responsibilities in maintaining cyber security[13]. This includes training on safe computing practices, password hygiene, and how to identify and report potential security incidents.

Incident detection and response: Establish mechanisms for detecting and responding to security incidents promptly. This involves implementing monitoring tools, intrusion detection systems, and incident response plans to minimize the impact of attacks and facilitate recovery[14].

Continuous monitoring and improvement: Regularly monitor and assess the effectiveness of implemented security controls. This includes conducting vulnerability assessments, penetration testing[15], and security audits to identify any gaps or weaknesses and make necessary improvements.

Compliance and regulatory adherence: Ensure compliance with relevant laws, regulations, and industry standards pertaining to cyber security[16]. This includes staying updated on changes to regulations and adapting security practices accordingly.

Survey Design:

The survey questionnaire will be designed to collect data on cyber security awareness and preparedness. The questionnaire will consist of a combination of multiple- choice, Likert scale, and open-ended questions. The questions will cover various aspects, including knowledge of common cyber threats, use of security measures and practices, training and education received, and perceived level of preparedness[17]. The survey will also gather demographic information to analyze any variations in awareness and preparedness based on factors such as age, gender, occupation, and organizational size.

Data Collection:

The survey will be distributed to a diverse sample of individuals and organizations. A combination of online platforms, email invitations, and physical distribution methods will be used to reach a wide range of participants. The data collection process will be conducted over a specified period to ensure a sufficient sample size for analysis. Reminders will be sent to maximize the response rate.

Data Analysis:

The collected data will be analyzed using statistical software to generate descriptive statistics and identify trends. Quantitative data, such as Likert scale responses, will be analyzed using measures such as means, frequencies, and percentages [18]. Cross-tabulations and chi-square tests will be performed to examine relationships between variables. Open-ended responses will be analyzed using content analysis to identify common themes and insights. The findings will be presented in a clear and concise manner, utilizing tables, charts, and graphs, to facilitate the interpretation of results.

Cyber Security Parameters

Cyber security parameters refer to the various factors or elements that are considered when assessing and implementing security measures to protect computer systems [19], networks, and data from cyber threats. These parameters can include:

1. **Confidentiality:** Ensuring that only authorized parties or organizations have access to sensitive information
2. **Integrity:** Maintaining the accuracy and consistency of data, ensuring it is not tampered with or modified without authorization.
3. **Availability:** Ensuring that systems and data are accessible and usable when needed, without disruption or downtime.
4. **Authentication:** Confirming the legitimacy of persons or entities making access attempts to systems or data.
5. **Authorization:** Granting appropriate permissions and privileges to authorized individuals based on their roles and responsibilities.
6. **Non-repudiation:** Providing evidence that a particular action or transaction was performed by a specific user, preventing them from denying their involvement.
7. **Risk assessment:** Identifying and evaluating potential vulnerabilities and threats to determine the level of risk and prioritize security measures.
8. **Incident response:** Establishing procedures and protocols to detect, respond to, and recover from security incidents or breaches.
9. **Encryption:** Protecting data by converting it into unreadable form, ensuring that only authorized parties can decrypt and access it.
10. **Security monitoring:** Continuously monitoring systems and networks for any suspicious activities or anomalies.

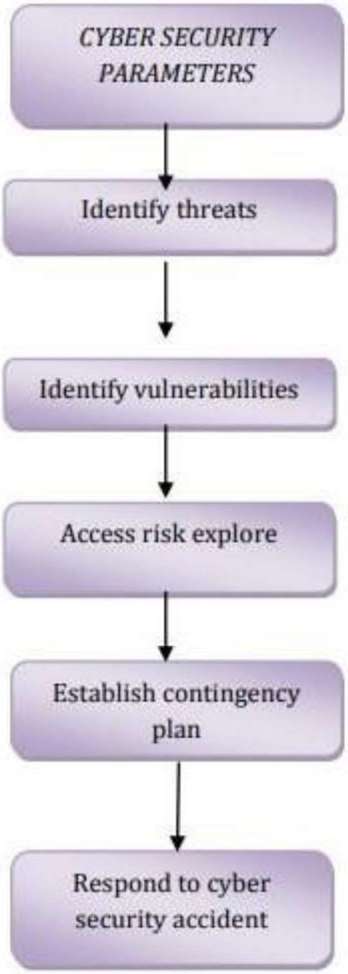
CYBER SECURITY PARAMETERS
Identify threats
Identify vulnerabilities
Access risk explore
Establish contingency plan
Respond to cyber security accident

Fig-1 Cyber Security Parameters

Results and Discussion

Demographic Analysis:

The demographic analysis will provide an overview of the participants' characteristics, such as age, gender, occupation, and organizational size. This analysis will help identify any variations in cyber security awareness and preparedness based on these factors[20]. For example, it may reveal that younger individuals have higher awareness levels compared to older individuals or that organizations with larger budgets have more robust security practices. The demographic analysis will provide valuable insights into the target audience and guide the development of tailored strategies for improving cyber security.

Level of Cyber Security Awareness:

This section will present the findings related to the level of cyber security awareness among the survey participants. It will include an analysis of their knowledge of common cyber threats, such as phishing, malware, and social engineering. The results will indicate the extent to which participants can identify potential threats and understand their implications. Additionally [21], the analysis may reveal any misconceptions or gaps in knowledge that need to be addressed through targeted awareness campaigns or educational programs.

Cyber Security Practices:

In this section, the survey findings regarding cyber security practices will be discussed. This includes the use of security measures and best practices by individuals and organizations. The analysis will examine the adoption of measures such as strong passwords, two-factor authentication, regular software updates, and data encryption. It will also assess participants' adherence to safe browsing habits and their awareness of potential risks associated with sharing personal information online[22]. The results will provide insights into the current state of cyber security practices and highlight areas for improvement.

Preparedness Measures:

This section will focus on the preparedness measures implemented by individuals and organizations to mitigate cyber threats. It will analyze the extent to which participants have implemented security measures, such as firewalls, antivirus software, and intrusion detection systems. The analysis will also evaluate the presence of incident response plans, data backup procedures[23], and employee training programs. The findings will shed light on the level of preparedness and help identify gaps that need to be addressed to enhance resilience against cyber-attacks.

Identified Gaps and Challenges:

This section will discuss the gaps and challenges identified through the survey analysis. It will highlight areas where participants have demonstrated lower levels of awareness or preparedness. For example, it may reveal a lack of awareness about emerging cyber threats or a limited understanding of the importance of regular software updates. The discussion will also address the challenges faced by individuals and organizations in implementing effective cyber security practices[24]. This may include factors such as budget constraints, limited access to training resources, or a lack of organizational commitment to cyber security. The identified gaps and challenges will serve as a basis for recommendations and strategies to improve cyber security awareness and preparedness.

Recommendations

Enhancing Cyber Security Awareness:

Based on the survey findings, it is recommended to focus on enhancing cyber security awareness among individuals and organizations. This can be achieved through targeted awareness campaigns that educate users about common cyber threats, such as phishing, malware, and social engineering [25]. These campaigns should emphasize the importance of safe browsing habits, strong passwords, and regular software updates. Additionally, raising awareness about emerging threats and providing resources for staying updated with the latest security practices will help individuals and organizations stay vigilant against evolving cyber threats.

Strengthening Cyber Security Preparedness:

To improve cyber security preparedness, organizations should prioritize the implementation of robust security measures. This includes regularly updating firewalls, antivirus software, and intrusion detection systems. Organizations should also establish incident response plans and conduct regular drills to ensure a prompt and effective response to cyber-attacks[26]. Additionally, data backup procedures should be implemented to minimize the impact of data breaches or system failures. By strengthening their preparedness measures, organizations can reduce the likelihood and impact of cyber-attacks.

Training and Education Programs:

Investing in training and education programs is crucial to improving cyber security awareness and preparedness. Organizations should provide regular training sessions to employees, covering topics such as recognizing and reporting suspicious emails, avoiding social engineering attacks, and maintaining good cyber hygiene practices[27]. Training programs should also be tailored to the specific needs of different departments and roles within the organization. Furthermore, individuals should be encouraged to pursue certifications and professional development opportunities in the field of cyber security to enhance their knowledge and skills.

Policy and Regulatory Considerations:

Governments and regulatory bodies should play an active role in promoting cyber security awareness and preparedness. They should develop and enforce regulations that require organizations to implement adequate security measures and regularly assess their cyber security posture[28]. Additionally, governments should collaborate with industry stakeholders to develop standardized frameworks and best practices for cyber security. Public- private partnerships can facilitate the sharing of information and resources to combat cyber threats effectively. Furthermore, governments should allocate resources to support research and development in the field of cyber security to stay ahead of emerging threats.

Conclusion

7.1 Summary of Findings:

In conclusion, the survey findings have provided valuable insights into the current state of cyber security awareness and preparedness among individuals and organizations. The demographic analysis has revealed any variations in awareness and preparedness based on factors such as age, gender, occupation, and organizational size. The analysis of cyber security awareness has highlighted the knowledge gaps and misconceptions that need to be addressed through targeted awareness campaigns and educational programs. The analysis of cyber security practices and preparedness measures has identified areas for improvement, such as the adoption of robust security measures and the implementation of incident response plans and data backup procedures.

6.2 Implications for Future Research:

The survey findings have significant implications for future research in the field of cyber security. Further studies can be conducted to explore the effectiveness of different awareness campaigns and training programs in improving cyber security practices. Additionally, research can be conducted to understand the impact of regulatory policies and frameworks on organizations' cyber security posture. Future research can also focus on evaluating the effectiveness of emerging technologies, such as artificial intelligence and machine learning, in enhancing cyber security measures. Furthermore, ongoing research is crucial to monitor the evolving threat landscape and identify new challenges and vulnerabilities that need to be addressed.

REFERENCES

[1] *Jitendra Jain et al, International Journal of Advanced Research in Computer Science, 8 (3), March-April 2017, 791-793*

[2] *International Journal of Computer Applications (0975 – 8887) Volume 111 – No 7, February 2015*

[3] *Recent Trends in Programming Languages ISSN: 2455-1821 (Online) Volume 4, Issue 2 www.stmjournals.com*

[4] *© The Author(s). 2018 Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License*

[5] *Cabaj et al. EURASIP Journal on Information Security (2018) 2018:10*

[6] *https://doi.org/10.1186/s13635-018-0080*

[7] *S. Bhutada and P. Bhutada, Application of Artificial*

[8] *Intelligence in Cyber Security: in IJERCSE, 2018, 5(4): 214-219*

[9] *P.V. Alberto, lecture, Topic: Application of Artificial Intelligence (AI) to Network Security‖, ITEC 625, University of Maryland, University College, Maryland, Mar. 2018.*

[10] *Avira, The Application of AI to Cybersecurity – An Avira White Paper, Germany, Avira Operation, 2017.*

[11] *S. A Panimalar, U.G. Pai and K.S. Khan, ―AI Techniques for Cyber Security‖, International Research Journal of Engineering and Technology, vol. 5, 3, pp. 122-124, Mar. 2018. Available: https://www.irjet.net [assessed May. 29, 2020]*

[12] *T.S. Tuang. Diep.Q. B, and Zelinka. I, Artificial Intelligence in the Cyber Domain: Offense and Defense: Symmetry, 2020, 12,410 available: www.mdp.com/journal/symmetry on [assessed Apr. 20, 2020]*

[13] *E. Kanal, Machine Learning in Cybersecurity: Carnegie Mellon University Software Engineering Institute, available*

[14] *onhttp://insights.sei.cnu.edu./sei_blog/2017/06/mac hine _learning_in_cybersecurity.html*

[15] *D. Selma, C. Huseyin and A. Mustafa, Application of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review, International Journal of Artificial Intelligence &Applications, vol. 6, issue 1, pp. 21-39, January 2015.*

[16] *T. Enn, ―Artificial Intelligence in Cyber Defense‖, in Proceedings of 3rd International Conference on Cyber Conflicts [ICCC], 7-10 June, 2011 Tallin Estonia.*

[17] *P. Dennis, A. Stuart, ―Global Challenges: Twelve risks that threaten human civilization, Global Challenges Foundation‖: 2015,Available: http://globalchallenges.org /wp-content/ uploads/12-Risks-with-infinite-impact.pdf [accessed Jun. 3, 2020]*

[18] *R. Stuart, D. Daniel, T. Max, __Research Priorities for Robust and Beneficial Artificial Intelligence'', AI Magazine, vol. 36, issue 4, pp. 105-114, Winter 2015*

[19] *National Science & Technology Council,*

[20] *―Artificial Intelligence and Cybersecurity: Opportunities and Challenges‖ Net. & Info.Tech R&D Sub-comtt and the ML & AI Sub-comtt, 2020.*

   a. *M. Shamiulla, Role of Artificial Intelligence in Cyber Security, International Journal of Innovative Technology and Exploring Engineering, vol. 9 issue 1 pp. 4628-4630, November 2019*

[21] *P. Pranav, ―Artificial Intelligence in cyber security‖, International Journal of Research in Computer Applications & Robotics, vol 4, 1, pp.1- 5, May 2016*

[22] *J. Kivimaa, A. Ojamaa, E. Tyugu. Graded Security Expert System. Lecture Notes in Computer Science, v. 5508. Springer, 2009, 279-286.*

[23] *B. Christain, D.A. Elizondo and T. Watson,*

[24] *—Application of artificial neural networks and related techniques to intrusion detection‖, World Congress on Computation Intelligence, pp 949- 954, 2010*

[25] *E. Tyugu, —Artificial Intelligence in Cyber Defense‖, International conference on Cyber Conflict, vol. 3, pp. 95-105, Tallinn, Estonia, Jan. 2011*

[26] *W. Nadine and K. Hadas, —Artificial Intelligence in Cybersecurity‖, Cyber, Intelligence, and Security, vol. 1, 1, pp. 103-119, Jan. 2017*

[27] *S. Dima, M. Robert, B. Zvi, S. Shahar and E. Yuval, —Using Artificial Neural Network to Detect Unknown Computer Worms‖, Neural Computing and Applications, vol.18, 7, pp. 663- 674, Oct. 2009*

[28] *E. H. Geoffrey, O. Simon and T. Yee-Whye, —A Fast Learning Algorithm for Deep Belief Nets‖, Neural Computation, vol. 18, no. 7, pp. 1527-1554, 2006*

[29] *V. Thomson, —Cyber Attacks Could be Predicted with Artificial Intelligence‖, iTechPost, www.itechpost.com/articles/1734 7/cyberattacks- predicted-artificial-intelligence-help.htm, Apr. 21, 2016 [Jun. 2, 2020]*

[30] *S. Franklin and A. Graesser, —Is It an Agent, or Just a Program? A Taxonomy for Autonomous Agents‖, Third International Workshop on Agent Theories, Architectures, and Languages, no. 3, pp. 21-35, 1997*

[31] *Y. Xia and L. Junshan, —A Security Architecture Based on Immune Agents for MANET‖, International Conference on Wireless Communication and Sensor Computing, no. , pp. 1- 5, 2010*