International Scientific Journal of Engineering and Management
Volume: 03 Issue: 05 | May – 2024
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
DOI: 10.55041/ISJEM01791

A STUDY ON THE EMPLOYEES' OPINION TOWARDS EFFECTIVENESS OF CYBER SECURITY MEASURES IN OMEGA HEALTHCARE.

*SUPRAJA K **Dr. H. MICKLE AANCY
*II MBA Student, Panimalar Engineering College, Chennai.
**Assistant Professor, Panimalar Engineering College, Chennai.

ABSTRACT

The study examines employee satisfaction and perceptions regarding cybersecurity measures at Omega Healthcare. It aims to assess management support, factors affecting security training, challenges in policy adherence, and suggests improvements. Using a mixed-methods approach, it combines surveys and interviews with a diverse sample of employees. Surveys gauge satisfaction levels and policy adherence, while interviews delve into experiences and suggestions. The findings aim to inform Omega Healthcare's cybersecurity strategy, promoting a culture of security awareness and compliance.

INTRODUCTION

Cybersecurity is the practice of protecting internet-connected systems such as hardware, software and data from cyberthreats. It's used byindividuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

In the rapidly evolving landscape of digital technology, ensuring robust cyber security measures has become imperative for individuals, organizations, and governments alike. The prevalence of cyber threats, ranging from data breaches and ransomware attacks to phishing scams and identity theft, underscores the critical need for proactive and comprehensive security strategies. This introduction will delve into the fundamentals of cyber security measures, exploring key concepts, challenges, and effective approaches to protect against cyber threats. Cyber security encompasses a broad range of practices and technologies designed to safeguard digital systems, networks, and data from unauthorized access, disruption, or damage. It involves protecting information assets and preventing cyber-attacks that exploit vulnerabilities in computer systems and networks.

ISSN: 2583-6129
DOI: 10.55041/ISJEM01791

REVIEW OF LITERATURE

Shekha Chenthara(2023), The proposed model stores only the encrypted hash of the records, proving effective in terms of data security, privacy, scalability, interoperability, and integrity while sharing and accessing medical records across the health chain network. **Ha Xuan Son(2023),** To show how well the approach manages security and privacy problems, it is put into practice in a real-world application. **Marialida Farah(2022),** The study plans to implement various Information Security Awareness interventions to address these issues.

Meikaign Qui (2022), The algorithm's performance on a smartphone platform is evaluated to prove efficiency. **Vijayalakshmi Saravanan(2022),** The framework combines technical mechanisms and environmental controls, demonstrating its ability to address common network security threats. **Abdullah T Alanazi (2021),** A unified approach is needed to enforce policies, modify behaviors, and adopt innovative practices to combat cyberattacks effectively. **Sabri Barbaria (2021),** This paper studies the usability of blockchain in healthcare and develops the Hyperledger Blockchain model, focusing on privacy concerns and patient consent integration in data-sharing operational controls. **Mohammed Alshehri (2021),** This distribution of medical data from IoMT and integrated devices, making it suitable for healthcare professionals and the healthcare industry. **Nehama Lewis (2021),** The study found that key data security personnel did not prioritize advanced cybersecurity technologies for funding or adoption. **Vasiliki Kelli (2021),** Blockchain access control component based on smart contracts for distributed access control to patient records and health data. **Steve Ahouanmenou (2020),** The study calls for more research in managerial and non-technical domains of information security and privacy. **Nehama Lewis (2020),** The study suggests guidelines to improve patient data security and reduce future data breaches by promoting cross-sectoral collaboration within the healthcare ecosystem. **Jong-Hwa Lee (2020),** The model's future improvement plans include reducing GPU and CPU resources. **Karuna S Bhosale (2020),** Cybersecurity involves protecting networks, devices, programs, and data from attacks, damages, and unauthorized access. **Menaka Muthuppalaniappan (2020),** Key COVID-19 cyber-security principles are outlined for both organizations and academic institution. **Abdullah Mohammed Alodaynan (2019),** This research explores penetration, attacker motives, methods, and effects on victims. **Sebastian Paul (2019),** The researchers also provide a proof of security in the symbolic model for the two PQC-based variants of OPC.

ISSN: 2583-6129
DOI: 10.55041/ISJEM01791

OBJECTIVES OF THE STUDY

- To assess the level of top management support for cybersecurity initiatives.
- To explore elements influencing security training and employee awareness of cybersecurity implementations.
- To identify challenges to employee adherence to cybersecurity policies.
- To make recommendations for improving the company's flexibility in cybersecurity measures.

NEED OF THE STUDY

The study on employee satisfaction with cybersecurity implementation at Omega Healthcare is vital for several reasons. Firstly, it helps assess the effectiveness of cybersecurity measures in safeguarding sensitive information, particularly in industries like healthcare. Secondly, employee satisfaction impacts productivity and retention rates. Understanding satisfaction levels fosters a culture of cybersecurity awareness and adherence, enhancing overall security. Positive satisfaction promotes employee engagement, while dissatisfaction may increase internal security risks. This study enables Omega Healthcare to refine cybersecurity strategies, prioritizing data protection and employee well-being effectively.

SCOPE OF THE STUDY

This study examines employee satisfaction with cybersecurity measures at Omega Healthcare, focusing on dimensions like top management support, communication, rewards, training, and awareness. It aims to understand how these factors influence overall satisfaction and perception. By analyzing management support, communication clarity, reward adequacy, and training comprehensiveness, it seeks insights to enhance satisfaction and engagement with cybersecurity. Anticipated findings will offer actionable recommendations to bolster Omega Healthcare's cybersecurity posture and resilience.

RESEARCH METHODOLOGY

The research design adopted in this study is Descriptive Research. Descriptive research is a research method describing the characteristics of the population or phenomenon studied. The primary data collection techniques used in this study is QUESTIONNAIRE METHOD. In this study, the major questionnaire technique used is Close Ended Questions. The sampling method used in this study is PROBABILITY SAMPLING. Probability sampling is a sampling technique

ISSN: 2583-6129
DOI: 10.55041/ISJEM01791

where a researcher selects a few criteria and chooses members of a population randomly. The sampling technique used in this study is Simple Random Sampling. The sample size for this study is determined using KREJCIE AND MORGON TABLE. The sample size for this study is 169, which is derived from the total number of employees in the organization, i.e., population(N) of 300. The collected data has been analyzed by the following statistical tool:

1) Mann-Whitney U-Test

2) Correlation

DATA ANALYSIS AND INTERPRETATION

MANN-WHITNEY U TEST

Hypothesis:

H0: There is no significant difference between the mean ranks of male & female with respect to the variables.

H1: There is a significant difference between the mean ranks of male & female with respect to the variables.

TABLE SHOWING U TEST SIGNIFICANCE WITH GENDER AS GROUPING VARIABLE

	Assess the level of satisfaction of top management support for cybersecurity initiatives	Explore elements influencing security training and employee awareness of cybersecurity implementations	To make recommendations for improving the company's flexibility in cybersecurity measures.	Identify challenges to employee adherence to cybersecurity policies
Mann-Whitney U	2639.500	2575.500	2675.500	2979.000
Wilcoxon W	8855.500	8791.500	8891.500	9195.000
Z	-1.924	-2.138	-1.806	-.798
Asymp. Sig. (2-tailed)	.054	.086	.071	.425

INTERPRETATION

The Mann – Whitney U test was conducted on the sample data, and it is found that the significance value (P value) for all the variables is more than 0.05 i.e., P>0.05. Therefore, the null hypothesis (H0) is accepted. Thus, there is no significant difference between the mean ranks of male & female with respect to the variables. So, the alternative hypothesis is rejected.

ISSN: 2583-6129
DOI: 10.55041/ISJEM01791

CORRELATION

Hypothesis

H0: The variables are not correlated with each other.

H1: The variables are correlated with each other.

TABLE SHOWING CORRELATION BETWEEN THE VARIABLES

Correlation

			Assess the level of satisfaction of top management support for cybersecurity initiatives	Explore elements influencing security training and employee awareness of cybersecurity implementations	To make recommendations for improving the company's flexibility in cybersecurity measures.	Identify challenges to employee adherence to cybersecurity policies
Spearman's rho	Assess the level of satisfaction of top management support for cybersecurity initiatives	Correlation Coefficient	1.000	.666**	.664**	.573**
		Sig. (2-tailed)	.	.000	.000	.000
		N	169	169	169	169
	Explore elements influencing security training and employee awareness of cybersecurity implementations	Correlation Coefficient	.666**	1.000	.721**	.662**
		Sig. (2-tailed)	.000	.	.000	.000
		N	169	169	169	169
	To make recommendations for improving the company's flexibility in cybersecurity measures.	Correlation Coefficient	.664**	.721**	1.000	.713**
		Sig. (2-tailed)	.000	.000	.	.000
		N	169	169	169	169
	Identify challenges to employee adherence to cybersecurity policies	Correlation Coefficient	.573**	.662**	.713**	1.000
		Sig. (2-tailed)	.000	.000	.000	.
		N	169	169	169	169

**. Correlation is significant at the 0.01 level (2-tailed).

INTERPRETATION

The correlation was conducted on the sample data, and it is found that the significance value (P value) for all the variables is less than 0.05 i.e., P<0.05. Therefore, the null hypothesis (H0) is rejected. The variables are highly correlated with each other.

ISSN: 2583-6129
DOI: 10.55041/ISJEM01791

FINDINGS

The employee demographic profile indicates a male majority of 65.7%, with 46.7% falling in the 20-40 age bracket and 55% holding Bachelor's Degrees. Experience-wise, 42.6% have 1-5 years with the company, while 39.1% earn Rs.20,000-Rs.50,000 monthly. In cybersecurity, 36% strongly affirm top management's commitment, with 54.4% agreeing concerns are addressed. Training effectiveness is questioned by 36% and 31%, while 26% feel prepared to identify threats. Confidence post-training stands at 23.7%. Communication clarity sees 59.2% feeling informed about updates, while 60.4% sense an encouraging cybersecurity culture. Statistical tests reveal significant age differences and a gender-satisfaction dependency, though variables correlate weakly, The R Square value, which is 0.07, indicates that approximately 7% of the variance in the dependent variable can be explained by the combination of these independent variables in the model.

SUGGESTIONS

Develop tailored cybersecurity training for various job roles and expertise levels, including general awareness sessions and specialized training for IT and data-handling personnel. Utilize interactive communication channels like intranet portals and forums for easy access to cybersecurity resources. Adapt security measures to suit different work environments and evolving business needs, while rewarding proactive cybersecurity behaviors. Regularly update incident response plans to ensure preparedness for breaches and launch awareness campaigns to educate employees about common threats and online security practices.

CONCLUSION

The study on "Employees' Opinion Towards Effectiveness of Cybersecurity Measures" reveals insights into employee perceptions. While satisfaction exists in some areas, significant gaps signal a need for improvement. Strengths include management commitment recognition, but concerns about training effectiveness and flexibility persist. Tailored training and awareness approaches are vital, with emphasis on continuous evaluation and improvement. Strategies include enhanced management engagement, tailored training, fostering collaboration, and incident response plans, all aimed at bolstering cybersecurity posture and fostering a resilient, aware organizational culture against evolving cyber threats.

ISSN: 2583-6129
DOI: 10.55041/ISJEM01791

REFERENCES

- Shekha Chenthara, Khandakar Ahmed, Hua Wang, Frank Whittaker, Zhenxiang Chen, "Healthchain: A Novel Framework on Privacy Preservation of Electronic Health Records Using Blockchain Technology" PLOSONE journal (2023).
- Ha Xuan Son, Minh Hoang Nguyen, Hong Khanh Vo, The Phuc Nguyen, "Toward An Privacy Protection Based on Access Control Model in Hybrid Cloud for Healthcare Systems" Advances in Intelligent Systems and Computing book series (AISC,volume 951) (2023).
- Marialida Farah, Samar Helou, Pascal Tufenkji, Elie El Helou, "Data Protection in Healthcare Research: Medical Students' Knowledge and Behavior" Advances in Informatics, Management and Technology in Healthcare (2022).
- Han Qiu, Meikang Qiu, Meiqin Liu, Gerard Memmi, "Secure Health Data Sharing for Medical Cyber-Physical Systems for The Healthcare 4.0" IEEE Journal of Biomedical and Health Informatics (Volume: 24). (2022).
- Shanying Zhu, Vijayalakshmi Saravanan, BalaAnand Muthu, "Achieving Data Security and Privacy Across Healthcare Applications Using Cyber Security Mechanisms" The Electronic Library, Vol. 38 (2022).
- Abdullah T Alanazi, "Clinicians' Perspectives on Healthcare Cybersecurity and Cyber Threats" Cureus (2021).
- Sabri Barbaria, M. C. Mont, E. Ghadafi, Halima Mahjoubi Machraoui, H. B. Rahmouni, "Leveraging Patient Information Sharing Using Blockchain-Based Distributed Networks" IEEE Access (2022).
- Mohammed Alshehri, "Blockchain-assisted Cyber Security in Medical Things Using Artificial Intelligence" Electronic Research Archive (2021).
- Nehama Lewis, Yaron Connelly, Gil Henkin, Max Leibovich, Adi Akavia, "Factors Influencing the Adoption of Advanced Cryptographic Techniques for Data Protection of Patient Medical Records" Healthcare informatics research (2021).
- Vasiliki Kelli, Panagiotis G. Sarigiannidis, Vasileios Argyriou, Thomas Lagkas, Vasileios Vitsas, "A Cyber Resilience Framework for NG-IoT Healthcare Using Machine Learning and Blockchain" ICC 2021 - IEEE International Conference on Communication (2021).
- Steve Ahouanmenou, Amy Van Looy, Geert Poels, "Information Security and Privacy in Hospitals: A Literature Mapping and Review of Research Gaps" Informatics for health & social care (2021).
- Nehama Lewis, Yaron Connelly, Gil Henkin, Max Leibovich, Adi Akavia "Factors Influencing the Adoption of Advanced Cryptographic Techniques for Data Protection of Patient Medical Records" Healthcare informatics research (2020).
- Jong-Hwa Lee, Jong-Wouk Kim, Mi-Jung Choi, "SSAE - DeepCNN Model for Network Intrusion Detection" 2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS) (2020).
- Karuna S Bhosale, Maria Nenova, Georgi Iliev, "A Study of Cyber Attacks: In the Healthcare Sector" Sixth Junior Conference on Lighting (Lighting) (2020).
- Menaka Muthuppalaniappan, Kerrie Stevenson, "Healthcare Cyber-attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health" International journal for quality in health care (2020).

ISSN: 2583-6129
DOI: 10.55041/ISJEM01791

- Abdullah Mohammed Alodaynan, Adwan Alownie Alanazi, "A Survey of Cybersecurity Vulnerabilities in Healthcare Systems" International Journal of ADVANCED AND APPLIED SCIENCES (2020).
- Sebastian Paul, Patrik Scheible, Friedrich Wiemer, "Towards Post-quantum Security for Cyber-physical Systems: Integrating PQC Into Industrial M2M Communication1" Journal of Computer Security (2019).
- Andreas Aigner, Abdelmajid Khelil, "A Benchmark of Security Metrics in Cyber-Physical Systems" IEEE International Conference on Sensing, Communication and Networking (SECON Workshops) (2019).
- Tiago Murer Furlanetto, Edimara Mezzomo Luciano, Odirlei Antonio Magnagnagno, Rafael Mendes Lubeck, "Information Security in Healthcare Supply Chains: An Analysis of Critical Information Protection Practices" Gestao & Producao (2019).
- Faisal Hussain, Syed Ghazanfar Abbas, Ghalib A Shah, Ivan Miguel Pires, Ubaid U Fayyaz, Farrukh Shahzad, Nuno M Garcia, Eftim Zdravevski, "A Framework for Malicious Traffic Detection in IoT Healthcare Environment" Sensors (Basel) (2018).

