2nd Edition 2023 SAKCON CAHO

A MIXED METHOD STUDY ON AWARENESS OF CYBERSECURITY AND DEVELOPMENT OF TRAINING MODULE IN A TERTIARY CARE HOSPITAL

Dr. Khusbu Sharma[1] , Dr Simran Dubey[1] , Ms Aileen J[2]

CAHO Committed to Safer Healthcare

INTRODUCTION

Cybercrime emerged in the late 1970s as the computer information technology (IT) industry took shape. (Kruse et.al ,2017)

Until 2016, cybersecurity was something on hold in the healthcare organizations. (Nunes et al. , 2021)

Cyber threats are increasing across all business sectors, with health care being a prominent domain. (Argyridou et al. ,2023)

Cybersecurity awareness in hospitals is crucial to protect patient data and sensitive medical information. (Choo et al. 2018)

Creating a comprehensive training module on cybersecurity for hospitals involves understanding the unique challenges and solutions in the healthcare sector. (Kuo et al.2020)

AIM AND OBJECTIVES

Aim : To assess the awareness of cyber security among healthcare workers and develop a training module

OBJECTIVES

- To identify factors related to cyber threats and data breaches
- To assess the cybersecurity compliance among healthcare workers.
- To recommend training module to improve the cyber awareness and cybersecurity in a tertiary care hospital

METHODOLOGY

1 Process mapping

Assessment of cyber security compliance by Observational study – 8 departments

2 Structured interviews

Staffs of the IT departments - 11 questions

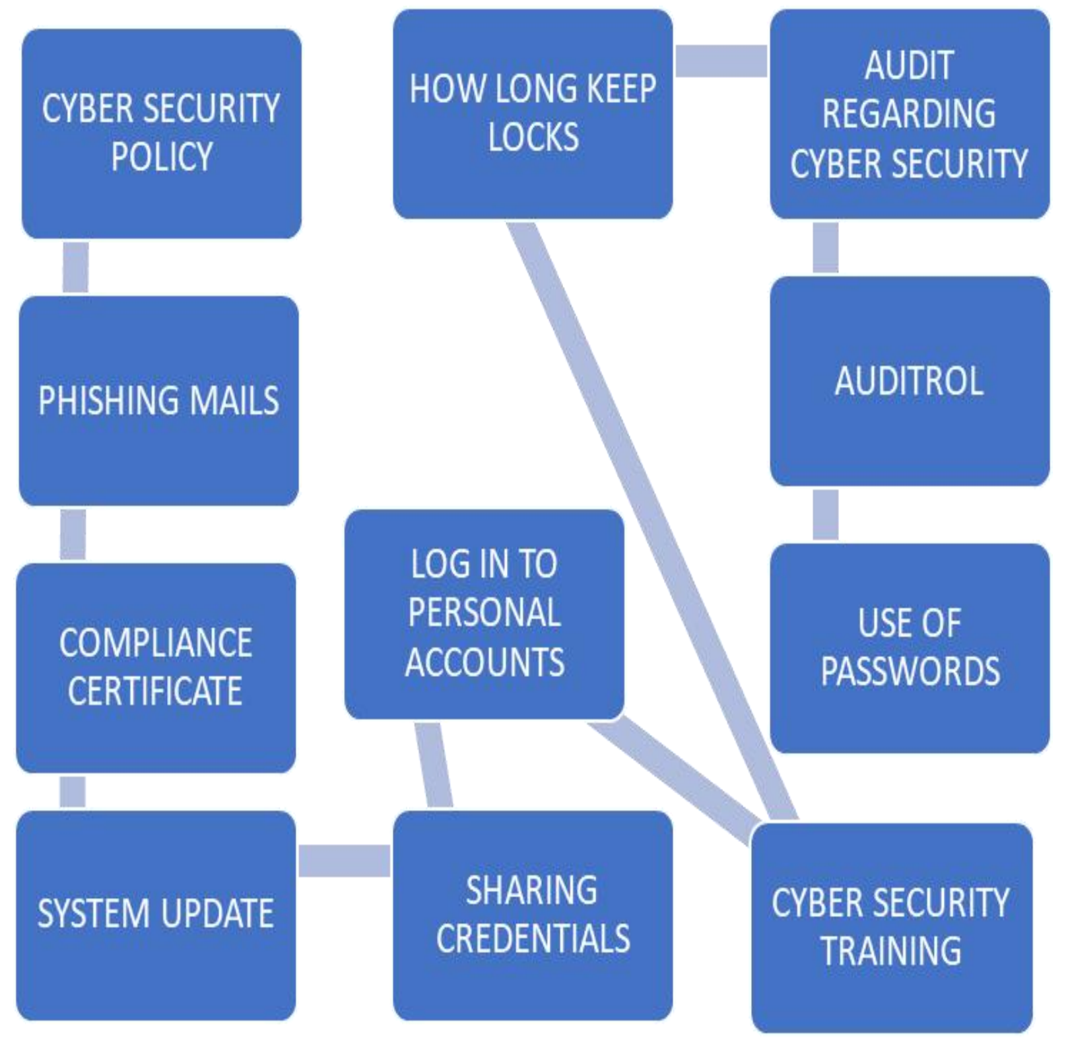
3 Nursing staff awareness survey

Nursing awareness on cyber security– 15 questions (Scaled)

4 Other healthcare workers awareness survey

Other workers awareness on cyber security– 12 questions (scaled)

RESULT AND DISCUSSION



(Based on the literature review 11 factors were identified)

- Among 12 IT staffs ; interview was conducted for 8 Staffs
- Based on the interviews there were 3 cybersecurity attacks in last 5 years, the last attack was in 2021 February.
- The other two was during COVID 19 epidemic in the year 2020.
- All the three attacks were ransomware and demanded payment through Bitcoins.
- Software in-use is ACCPAC &VnC.
- Currently no training given on cybersecurity for all the staff

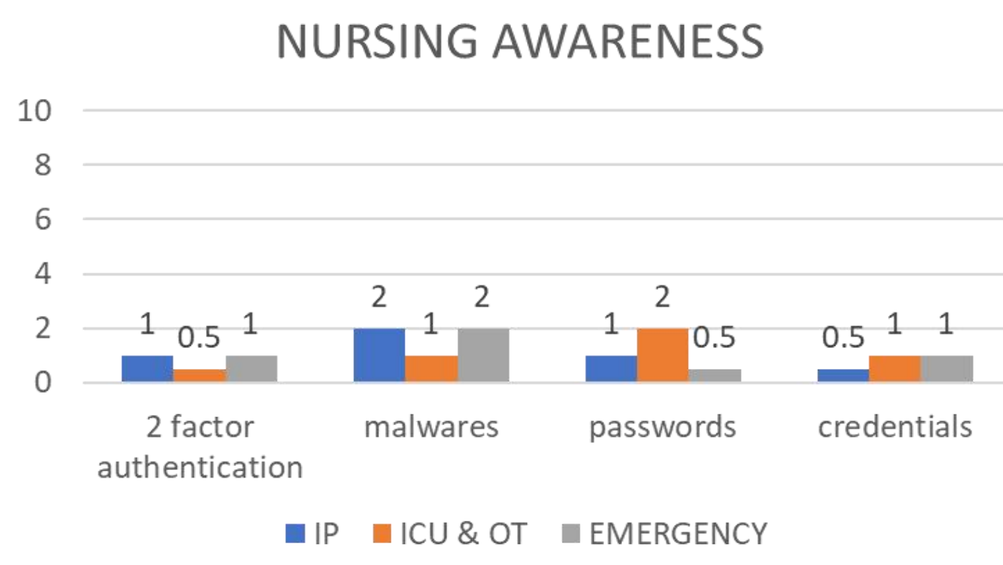
Checklist data analysis

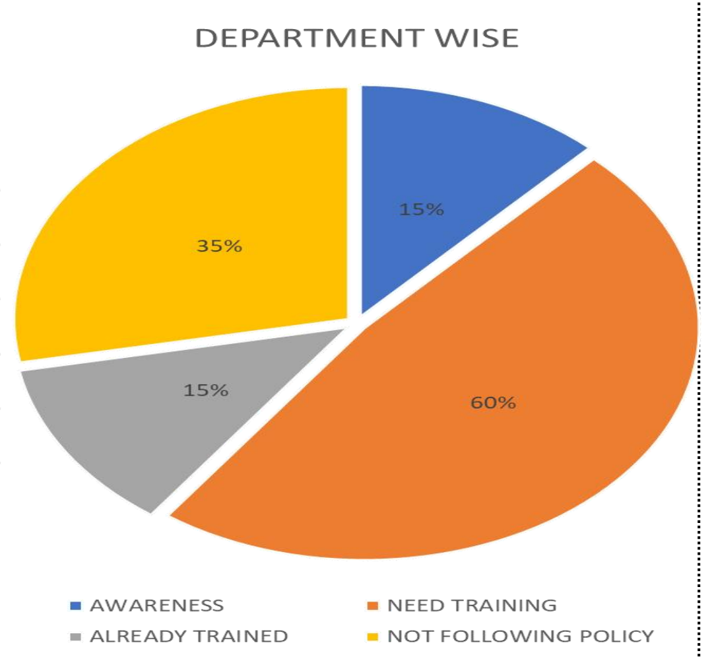
50% of healthcare workers are not following the cybersecurity policy

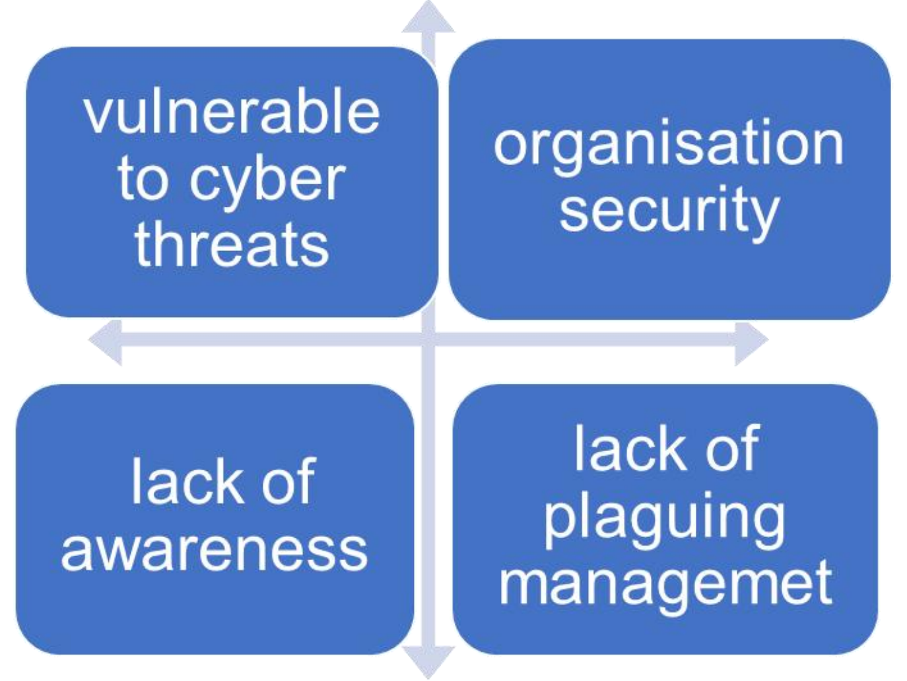
60 % of healthcare workers felt there is a need for training

85% of the healthcare workers are not aware cyber security threats like Phishing mails , sharing credentials.

Qualitative data analysis of interview







(Factors affecting cybersecurity)

PLAN FOR TRAINING MODULE

FREQUENCY	TARGET POPULATION	VULNERABLE GROUPS	COVERED TOPICS
1 SEPTEMBER 60 min	NURSING DEPARTMENT	NURSING DEPARTMENT	ENCRYPTION METHODS
1 JANUARY 60 min	BILLING DEPARTMENT	BILLING DEPARTMENT	PHISHING MAILS
1 MAY 120 min	IT DEPARTMENT	IT DEPARTMENT	ROUTE OF VIRUSES AFFECTS SYSTEM OR SERVERS
1 SEPTEMBER 30 min	ACCOUNT/FINANCE DEPARTMENT	ACCOUNT/FINANCE DEPARTMENT	STRONG PASSWORD AND FREQUENCY OF CHANGING THE PASSWORDS
1 JANUARY 180 min			MALWARES: RANSOMWARE VIRUSES, TROZEN VIRUSES

DISCUSSION

The incident highlighted the significance of cybersecurity awareness and training for healthcare personnel. WannaCry Ransomware Attack **(2017): The WannaCry ransomware attack** targeted hospitals and other organisations worldwide.

The **Cedars-Sinai Medical Centre** in the **United States** encountered a data breach that exposed patient information due to a **phishing attack in 2020**

The **2020 AIIMS Rishikesh Ransomware Attack:** According to reports, the All India Institute of Medical Sciences (AIIMS) in Rishikesh encountered a ransomware attack in 2020, which disrupted hospital systems and patient services.

The **result is similar** to the other cases **in India and international** healthcare organisation.

CONCLUSION

Pay attention to create awareness among employees for cybersecurity

Training healthcare professionals on cybersecurity

Reinforce the knowledge and skills required to protect patient data and hospital systems effectively.

To comprehend the risk associated with cyber attacks and necessary precautions.

REFERENCES

- Kuo, A. M. H., Hsu, C. H., & Nguyen, T. T. (2020). Developing and Evaluating a Cybersecurity Training Module for Healthcare Professionals. Health Informatics Research, 26(3), 178-185. doi:10.4258/hir.2020.26.3.178
- https://www.bmj.com/content/358/bmj.j3179#:~:text=It%20is%20one%20of%20the%20most%20targeted%20sectors,valuable%20data%2C%20and%20it%20is%20a%20soft%20target.
- https://content.iospress.com/articles/technology-and-health-care/thc1263
- https://pubmed.ncbi.nlm.nih.gov/37498644/#:~:text=Conclusions%3A%20The%20proposed%20CH%20methodology,related%20to%20health%20care%20employees.
- https://www.sciencedirect.com/science/article/pii/S1877050921001563
- Choo, K. K. R., Reddick, C. G., & Burke, G. B. (2018). Examining healthcare professionals' cybersecurity awareness and hygiene. Health Informatics Journal, 24(4), 2437-2447. doi:10.1177/1460458217737073