International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 13 Issue 10, October -2023,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.202| Thomson Reuters ID: L-5236-2015

HEALTH CARE WORKERS' INFORMATION SECURITY AWARENESS AND BEHAVIORS AT PUBLIC HEALTH HEALTHCARE CENTRES

VISWANATHAN B

(Research Scholar)

Dr. Lalit Kumar Khatri (Professor)

(Research Supervisor)

Glocal School of Technology And Computer Science

Abstract

This study aimed to help policymakers identify the most susceptible parts of the population and prioritize infrastructure and training expenditures by investigating the information security habits of public health professionals. Individuals employed by Indian public health care organizations were asked to fill out a paper-based, cross-sectional survey that was anonymous. To determine the degree to which each professional complies with appropriate cybersecurity practices, data was collected on their role, experience, work environment, cybersecurity practices, and understanding. This data was then used to compute their cybersecurity score. According to the findings, those with greater work experience had a better level of compliance with best practices for cybersecurity. Surprisingly, as compared to doctors, nurses show more proficiency in cybersecurity. Our research offers some suggestions for improving cybersecurity education for healthcare workers. With so many other pressing matters vying for doctors' time and focus, it is imperative that they get sufficient cybersecurity training.

Keywords: health information technology; public health sector; cybersecurity

1. Introduction

One's mental image of cybersecurity is a scenario from a Hollywood film: a server room guarded by lasers, a cornucopia of flashy technology, exposed cables, encryption, and a cool hero banging on a laptop keyboard to generate a smooth flow of green-on-black programming gibberish. This is the typical mental image of cybersecurity. The fact of the matter is that the digital and technological aspects of cybersecurity are not the only ones that are susceptible to being readily hacked upon. There is a great deal more. According to **Blanke and McGrady (2016),** one of the most prevalent types of breaches is the inadequacy of the physical security measures that are employed to secure information

technology assets that are portable. Other examples of this sort of breach include flash drives. Additionally, this is underlined in the criteria for health IT certification. Concerns regarding the hazards associated with user behavior in relation to cybersecurity are another factor that is usually ignored. Recent study indicates that the majority of information security issues arise as a result of workers of an organization either being unaware of or failing to appreciate the appropriate security rules and standards **(Solomon and Brown, 2021).** Phishing is one example of the expanding amount of fraudulent activities that are aimed at unwary people rather than information technology systems **(Jalali et al., 2020).**

According to **Kruse et al.'s (2020)** research, the cybersecurity of the healthcare industry is badly deficient in comparison to that of other businesses. Most hospitals and clinics in today's world would be unable to function properly without the utilization of health information technology (HIT). According to data that were published not too long ago **(Nifakos et al 2020),** cybercrime, which may lead to the compromise of protected health information, is a persistent concern for health care facilities, particularly hospitals. Despite the fact that the direct and indirect expenses of a breach vary in today's world, the average cost of a compromised health care record is more than 400 USD per record. One of the primary reasons for the majority of breaches is the acts and negligence of those who offer medical treatment.

When we talk about cybersecurity, we are referring to the process of preventing computer systems, networks, and data from being breached or exposed to various types of cyberattacks. The United States Food and Drug Administration (FDA) provided a more specific definition of cybersecurity by include the prevention of any illegal alteration, misuse, or denial of use of personal information that has been transported from one device to another external one. This was done in order to ensure that the information is not affected in any way. Cybersecurity threats can originate from both internal and external sources, with human error being a contributing element in some of the cyberattacks that occur. The information security policies, regulations, laws, and processes of a great number of firms are neglected, which results in human errors (**Fernández-Alemán 2015).**

Objective of study

The purpose of the study is to examine healthcare workers' cybersecurity knowledge and practices in the public health setting.

2. Methodology

A cross-sectional, paper-based survey was distributed among 350 healthcare professionals working in public health care facilities in India. The survey assessed demographic factors such as gender, age, years of experience, and job roles (physicians, nurses, and support staff). It also collected data on internet usage behaviors and security practices.

The cybersecurity awareness and behavior of respondents were measured using a Likert scale (1 = Strongly Disagree, 5 = Strongly Agree) across several key areas:

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 13 Issue 10, October -2023,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.202| Thomson Reuters ID: L-5236-2015

1. Knowledge of security policies
2. Secure internet and intranet usage
3. Protection of patient health information
4. Reporting of security incidents

A composite cybersecurity score (ranging from 0 to 10) was calculated based on participants' responses to the 16 security-related questions.

3. Results and analysis

Measure	Category	Frequencies	Percentage (%)	Mean	Std. Deviation
Gender	Female	185	53	-	-
	Male	165	47	-	
Role of Participants	Physician	140	40	-	-
	Clinical Staff	70	20	-	
	Nurses	105	30	-	
Security Awareness and Behaviors	Knowledge of Policies			4.2	0.77
	Internet/Intranet Use			3.9	0.60
	Patient Info Protection			3.5	0.57
	Incident Reporting			3.1	0.71
Amalgamated Security Score	Physician (8+ years)			6.0	
	Clinical Staff (8+ years)			6.8	
	Nurses (8+ years)	-		7.0	

Gender Distribution: The participant pool exhibited a nearly equal distribution of males and females, with a little majority of female participation.

Role of Participants: The primary participants were physicians, succeeded by nurses and clinical staff. This job variety offers a comprehensive perspective on the security behaviors of healthcare workers.

Security Awareness: The survey reveals a usually high understanding of security regulations and internet usage behaviors. Nevertheless, a significant deficiency in event reporting indicates the necessity for enhancing the reporting culture and system.

Impact of Experience and Role: The influence of experience and role: Participants with over 8 years of experience, especially nurses, demonstrated superior compliance with security measures, whereas physicians exhibited the lowest adherence to security rules, perhaps due to their clinical responsibilities. This indicates a necessity for focused efforts to enhance security procedures across various positions.

4. Discussion

The findings of this study highlight significant variations in the cybersecurity awareness and behaviors of healthcare professionals in public health care facilities in India. It was observed that healthcare professionals, particularly nurses, displayed higher levels of cybersecurity awareness compared to physicians. This discrepancy could be attributed to the varied focus of different professional roles, where physicians are more likely to prioritize clinical tasks over cybersecurity measures due to their heavy cognitive load and time constraints. In contrast, nurses, whose roles involve extensive interaction with digital tools for patient care and data entry, may develop better cybersecurity practices over time.

The analysis further demonstrates a positive correlation between years of work experience and adherence to cybersecurity protocols. Professionals with more than eight years of experience showed significantly higher compliance with secure practices, emphasizing the need for continuous on-the-job training to foster secure behaviors. However, there remains a notable gap in the reporting of security incidents, which is a critical area for improvement. This suggests a need for organizational culture shifts, where healthcare institutions should promote a more proactive attitude towards incident reporting, without fearing blame or reprimand.

Interestingly, while knowledge of security policies was generally high among respondents, the actual implementation of these policies, especially in secure internet usage and protection of patient health information, lagged slightly behind. This gap between knowledge and practice indicates that while awareness exists, behavioral adherence to cybersecurity protocols needs reinforcement through more targeted training programs and clear communication of the consequences of non-compliance.

5. Conclusion

This study has provided valuable insights into the cybersecurity awareness and behaviors of healthcare professionals in public health facilities in India. The findings suggest that experience plays a critical role in the adherence to good security practices, with more experienced professionals displaying better

compliance. Furthermore, the study revealed that nurses tend to exhibit higher cybersecurity aptitude compared to physicians, highlighting a potential area where targeted training for physicians could mitigate vulnerabilities.

Key recommendations include implementing ongoing cybersecurity training that is tailored to the unique needs and time constraints of different healthcare roles, with a particular focus on encouraging physicians to integrate security practices into their clinical routines. Moreover, there is a need to cultivate a stronger culture of incident reporting within healthcare organizations to address the current gaps in this area.

In conclusion, improving cybersecurity in healthcare requires a multi-faceted approach, combining education, culture shift, and policy enforcement, ensuring that all healthcare professionals, regardless of role or experience level, contribute to a more secure digital environment.

Reference

Blanke, S. J., & McGrady, E. (2016). When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. *Journal of healthcare risk management*, *36*(1), 14-24.

Solomon, G., & Brown, I. (2021). The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management*, *34*(4), 1203-1228.

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). Why employees (still) click on phishing links: investigation in hospitals. *Journal of medical Internet research*, *22*(1), e16775.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1-10.

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), 5119.

Fernández-Alemán, J. L., Sánchez-Henarejos, A., Toval, A., Sánchez-García, A. B., Hernández-Hernández, I., & Fernandez-Luque, L. (2015). Analysis of health professional security behaviors in a real clinical setting: An empirical study. *International journal of medical informatics*, *84*(6), 454-467.

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 13 Issue 10, October -2023,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.202| Thomson Reuters ID: L-5236-2015

DECLARATION

I as an author of this paper / article, hereby declare that paper submitted by me for publication in the journal is completely my own genuine paper. If any issue regarding copyright/ patent/ other real author arises. The publisher will not be legally responsible. If any of such matters occur publisher may remove my content from the journal website/ updates. I have resubmitted this paper for the publication, for any publication matters or any information intentionally hidden by me or otherwise, I shall be legally responsible.

Name: Viswanathan B