International Journal in IT & Engineering (IJITE)
Volume 10 Issue 12, Dec 2022 ISSN: 2321-1776 Impact Factor: 7.256
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

AN ANALYSIS OF VARIOUS HUMAN FACTORS IN CYBERSECURITY ADHERENCE FOR ENHANCING SECURITY PRACTICES

Viswanathan B
(Research Scholar)
Dr. Lalit Kumar Khatri (Professor)
(Research Supervisor)
Glocal School of Technology and Computer Science

Abstract

Cybercriminals target healthcare institutions, among others, and recent statistics show that human error is still the root cause of more than 85 percent of data breaches. Given the inherent human aspect in healthcare IT infrastructure, this study thoroughly investigated how psychosocial cultural and occupational variables influence security behavior in a conventional hospital setting. We used a quantitative technique, surveying healthcare workers online using a questionnaire, to get their feedback. Drawing on prior review work, a wide variety of constructs were chosen from aspects of the workplace, culture, social life, and psychology. To comprehensively examine the gaps in healthcare staff's knowledge, attitude, and behavior regarding information security (IS), they were linked to certain security practices. The study found that the risk of IS conscious care behavior (ISCCB) is positively correlated with work emergency (WE). Information security knowledge (ISK) and information security attitude (ISA) risk were inversely connected with agreeableness, whereas ISCCB risk was positively correlated with conscientiousness. These results lay the groundwork for future research into the use of innovative technology in conjunction with intrinsic and extrinsic motivation strategies to reduce the prevalence of hazardous behaviors associated with IS and to promote more self-aware approaches to care security.

Keywords: Cyber Security; Human Factors; information security (ISK) knowledge; IS conscious care behavior (ISCCB)

1. Introduction

In certain cases, hospitals that have completely integrated electronic health record (EHR) systems may refer to these systems as paperless or folder-less systems during their operations. For the purpose of providing medical treatment to patients, hospitals that have implemented paperless systems do not make use of any physical paperwork or files. According to **Hossain, Quaresma, and Rahman (2019),** the electronic health record system is responsible for handling all of the patient-related duties that are performed at the healthcare facility. These tasks include the documentation of outpatient and inpatient procedures, diagnostic and therapeutic procedures, referrals, and test orders connected to patients. It is hard to overestimate the benefits of paperless systems, which include improved clinical decision support, more efficient administration of patients' information, and a reduction in the amount of physical space required to keep medical data **(Dagliati, et al., 2021).**

When it comes to cyber security events that take place after the fact and have an impact on information systems, healthcare systems are among the most common targets. This has been caused by a number of different factors. Historically, the focus of information security solutions has been on technical measures such as the setup of firewalls, the establishment of demilitarization zones, the implementation of intrusion detection and prevention systems, authentication, and authorization. Nevertheless, the human component of information systems management, which is sometimes referred to as the "human firewall," has not been acknowledged despite the fact that it has a significant role in reducing security threats **(Wiley, McCormac, & Calic, 2020).** In addition, fraudsters consider the healthcare industry to be an ideal target because of the level of urgency with which healthcare personnel are required to gather patient information. As an illustration, in the event that ransomware were to attack the healthcare industry, the authorities would gladly pay the demanded amount in order to promptly recover patient information.

According to **Pollini et al. (2022),** breaches in healthcare security can be triggered by a wide range of human factors. Personal, occupational, social, cultural, and psychological factors are some examples of these **(Yeng et al. 2019).** Other examples include cultural and social components. Furthermore, the assessments are not always exhaustive, which provides opportunity for human mistake. Researchers in the field of security usually look at these elements in an effort to enhance security procedures. However, the evaluations are not always complete. As an illustration, **Anwar et al. (2017)** investigated the ways in which gender plays a role in the conduct of security operations. The study did not take into consideration other characteristics, such as those that were associated with the workplace, despite the fact that it was quite important. This means that issues pertaining to gender inequalities among healthcare personnel would be recognized and addressed if the findings of Anwar et al. are taken into consideration in order to enhance security procedures in a typical hospital. However, we will not address problems that apply to

other parts of the human factor when it comes to this discussion. **Nifakos et al. (2021)** state that as a result of this, there is a possibility that there is a security flaw in the manner that the personnel handles security. Through the utilization of a descriptive methodology, this study contributed to the reduction of the gap by conducting an exhaustive analysis of a wide range of parameters, which included personal, occupational, social, cultural, and psychological elements. This purpose of the study is to assess how several human factors—psychological, social, cultural, and occupational—affect healthcare workers' cybersecurity practices.

2. Methodology

The hospitals and volunteers were recruited using a random selection method. To begin, we sent an invitation to participate in the study to healthcare facilities that had implemented "folder-less" systems. A small number of Ghanaian medical centres willingly participated in the research. The research did not provide the names or locations of these facilities due to ethical, privacy, and security concerns; nevertheless, ethical approval had already been acquired. The next step was to establish a system of liaisons between the hospitals' administrative and medical directors and research coordinators. The survey was extended to the healthcare personnel who had already established multimedia. Consequently, the online questionnaire link was sent around the network, and those who gave their approval to the research went on to fill it out.

3. Results

The study focused on three key areas:

- Information Security Knowledge (ISK): Understanding of cybersecurity protocols.
- Information Security Attitude (ISA): Feelings and attitudes towards complying with cybersecurity.
- Information Security Conscious Care Behavior (ISCCB): Actual practices related to security, such as logging off systems or managing passwords.

Table 1.1 shown the responses of participants on behaviour, attitude and knowledge

Measure	Mean	Std. Deviation
Information security knowledge (ISK) risk	1.40	0.38
Information security attitude (ISA) risk	1.75	0.46
Information security self-reported conscious care behavior (ISCCB) risk	2.55	0.39

The findings from the table shown that

Knowledge (ISK): Healthcare staff scored low, with an average of 1.40, suggesting they are not fully aware of the security risks.

Attitude (ISA): The attitude towards cybersecurity was slightly better, with a mean of 1.75, showing that staff feel somewhat confident about security measures.

Behavior (ISCCB): The actual security behavior had a mean score of 2.55, indicating that risky security practices occur more frequently than expected.

4. Discussion of results

Cybersecurity practices among healthcare employees using EHR were examined in this research to determine the impact of psychological, social, cultural, and work-related human variables. Several significant connections were identified by the results, which provide light on the ways in which these characteristics influence security practices in hospital settings.

It appears that in stressful circumstances, healthcare workers are more prone to put patient care ahead of security standards, as there is a positive association between work emergencies (WE) and "information security conscious care behavior (ISCCB)". In the healthcare industry, where quick access to patient information is essential, this might cause security measures to fail in times of crisis.

Additionally, the study discovered a positive correlation between conscientiousness and ISCCB risk, suggesting that professionals who are more meticulous in their work are more likely to adhere to better security standards. Those who are more agreeable may downplay security risks or comply with risky behaviors to keep the peace in the workplace, since agreeableness was found to have a negative correlation with both information security knowledge (ISK) and information security attitude (ISA).

These results highlight the need to address human elements in cybersecurity alongside technological ones. In their haste to help patients, healthcare workers, particularly in an emergency, run the risk of exposing sensitive information. Professionals' reactions to security threats can be heavily influenced by inherent attributes like agreeableness and conscientiousness.

5. Conclusion

This study demonstrated that human factors significantly affect cybersecurity behaviors in healthcare settings. In particular, work-related emergencies and personal characteristics such as conscientiousness and agreeableness play important roles in shaping professionals' security practices. These insights suggest that cybersecurity training in healthcare should be tailored to address these factors, emphasizing the importance of security even in high-pressure situations.

Future strategies should include both intrinsic (personality-based) and extrinsic (work-environment-based) motivations to encourage better adherence to security protocols. Additionally, organizations should explore combining these strategies with advanced technological solutions to minimize risks associated with human factors. By addressing both human and technical aspects, healthcare institutions can improve overall security and better protect sensitive patient information.

Reference

Hossain, A., Quaresma, R., & Rahman, H. (2019). Investigating factors influencing the physicians' adoption of electronic health record (EHR) in healthcare system of Bangladesh: An empirical study. *International Journal of Information Management*, *44*, 76-87.

Dagliati, A., Malovini, A., Tibollo, V., & Bellazzi, R. (2021). Health informatics and EHR to support clinical research in the COVID-19 pandemic: an overview. *Briefings in bioinformatics*, *22*(2), 812-822.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & security*, *88*, 101640.

Yeng, P. K., Yang, B., & Snekkenes, E. A. (2019). Healthcare staffs' information security practices towards mitigating data breaches: a literature survey. *pHealth 2019*, 239-245.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437-443.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*, *24*(2), 371-390.

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.

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