Journal of Public Health and Pharmacy
2775-4952 (Online - Elektronik)
Research Articles Open Access

Hospital Size and Cybersecurity Practices: Evaluating Nurses' Awareness in Indonesia

Irwandy Irwandy[1,2]*, Adelia U. Ady Mangilep[1], Rini Anggraeni[1], Noer Bahry Noor[1], Andi Niartiningsih[3], Nur Latifah[4], Andi Azisah Bari'ah[4]
[1]Faculty of Public Health, Hasanuddin University, Makassar 90245, Indonesia
[2]Hasanuddin University Hospital, Hasanuddin University, Makassar 90245, Indonesia
[3]Faculty of Health Science, Cokroaminoto University, Makassar 90245, Indonesia
[4]Center for Health Service Management Studies, Faculty of Public Health, Hasanuddin University, Makassar 90245, Indonesia

***Corresponding Author**: E-mail: wandy_email@yahoo.co.id

ARTICLE INFO

Manuscript Received: 19 Nov, 2024
Revised: 05 Mar, 2025
Accepted: 12 Mar, 2025
Date of publication: 02 Oct, 2025
Volume: 5
Issue: 3
DOI: 10.56338/jphp.v5i3.6412

KEYWORDS

Cybersecurity;
Nursing;
Healthcare Systems;
Knowledge;
Attitudes;
Practices

ABSTRACT

Introduction: This study aimed to evaluate nurses' knowledge, attitudes, and practices (KAP) regarding cybersecurity in healthcare settings, focusing on variations across hospitals of different sizes. Cybersecurity is critical in the digitalization of healthcare, yet gaps in awareness and training persist, particularly in developing countries. With increasing cyber threats targeting healthcare institutions globally, this study seeks to address the underexplored role of nurses in safeguarding hospital information systems.
Methods: This cross-sectional study was conducted in three government hospitals in Makassar, Indonesia, from [start month/year] to [end month/year]. A total of 331 nurses participated, representing hospitals of varying organizational sizes and bed capacities. Data were collected using structured questionnaires, assessing KAP related to cybersecurity. Ethical approval was obtained from [name of ethics committee], and written informed consent was secured from all participants. Data were analysed using descriptive and inferential statistics, with significance set at $p < 0.05$.
Results: The study revealed significant gaps in nurses' cybersecurity knowledge, attitudes, and practices. Awareness of hospital cybersecurity policies was low (43.2%), particularly in larger hospitals. Hospital 3, the smallest, exhibited higher awareness (59.0%) compared to Hospital 1 (35.8%) and Hospital 2 (39.6%) ($p = 0.03$). Risky behaviours, such as using personal devices for sensitive data transfer, were prevalent (77.0%), with the highest incidence in larger hospitals. Statistical analyses confirmed significant variations in cybersecurity KAP based on hospital size and organizational complexity.
Conclusion: This study highlights the critical need for targeted cybersecurity training programs, particularly for nursing staff in larger hospitals, through raising awareness of social engineering attacks, email scams, and infection detection. By addressing gaps in awareness and practices, hospitals can enhance data protection and mitigate risks. Future research should explore tailored interventions and organizational factors influencing cybersecurity in healthcare systems to inform global health policies.

Publisher: Pusat Pengembangan Teknologi Informasi dan Jurnal Universitas Muhammadiyah Palu

INTRODUCTION

Cybersecurity in healthcare is increasingly critical as hospitals and healthcare institutions adopt digital systems to manage patient data and optimize operations. While these technological advancements improve healthcare efficiency, they also introduce substantial risks to data security. Cyber threats such as data breaches, ransomware attacks, and social engineering continue to disrupt hospital information systems and compromise patient privacy. This issue is particularly complex in developing countries, where resources for cybersecurity awareness and training are often limited (1,2). The health sector is indeed a major target for cybercriminals, with ransomware attacks in this industry increasing by 650% in 2022 compared to the previous year. Costs resulting from health data breaches also rose significantly, from US$7.13 million in 2020 to US$9.23 million the following year, representing an increase of 29.5%.

Although various cybersecurity measures, such as data protection policies, antivirus software, and firewalls, have been implemented in hospitals to mitigate these risks, human factors remain a major challenge. Nurses, as primary users of hospital digital systems, play a crucial role in ensuring the security of patient data. Given their pivotal role in patient care and technology usage, nurses are uniquely positioned to safeguard data and report cybercrimes(3). Studies indicate that Nurses' knowledge and awareness of cybersecurity directly influence the risk of data breaches and cyber-attacks (4,5).

The most effective solution to enhance cybersecurity in hospitals involves a combination of technical security measures and targeted security awareness training for healthcare personnel(6,7). However, cybersecurity training often focuses on IT or administrative staff, with limited emphasis on frontline medical staff, particularly nurses. Moreover, nurses' perception of cybersecurity may be secondary to their primary patient care responsibilities, leading to potential gaps in their preparedness for cyber threats.

This study aims to evaluate nurses' knowledge, attitudes, and practices regarding cybersecurity in three government hospitals in Makassar, Indonesia. Additionally, it explores the variation in knowledge, attitudes, and practices across hospitals based on hospital size and bed capacity. It is essential to examine these variations because the challenges faced by hospitals of different sizes may vary significantly. Larger hospitals, with more complex organizational structures and resources, may encounter difficulties in maintaining consistent cybersecurity awareness and training across their staff. In contrast, smaller hospitals may have more centralized control, which could facilitate more focused cybersecurity training and policy implementation. Understanding how the size and organizational structure of a hospital influence cybersecurity practices is crucial for tailoring interventions that address the unique needs of each institution.

The results of this study are expected to fill existing gaps in the literature, particularly regarding the role of nurses in hospital cybersecurity. By examining how hospital size influences cybersecurity knowledge and practices among nurses, this research aims to provide a foundation for developing more effective training programs and policies, particularly in government hospitals in Indonesia. Furthermore, the study aligns with global health priorities, such as those outlined by the WHO (1,8), by contributing to improving healthcare cybersecurity practices and safeguarding patient data in a rapidly digitalizing healthcare environment.

METHOD

A comprehensive cybersecurity framework is essential for organizations to effectively manage and mitigate cyber threats. Such a framework integrates various components that address the multifaceted nature of cybersecurity, including technological, human, and organizational aspects. This study adopts a cross-sectional survey design to investigate cybersecurity practices from a human perspective among nurses in hospitals. This study used total sampling, and all provincial government hospitals located in South Sulawesi, Indonesia, were sampled. A total of 331 nurses participated in the study. Participation was voluntary, and each respondent provided informed consent prior to completing the survey. No time limits were imposed for completing the questionnaire, and participants were not offered any compensation or incentives.

To assess individual perspectives on cybersecurity, we developed a modified survey instrument to measure information security behaviours, drawing from established instruments in prior studies. The instrument comprised three key components: Knowledge(7,9), Attitudes(7), and Practices(7,9–14). The Knowledge component included items related to Awareness of Cybersecurity Policies, Recognition of Security Threats, Understanding of Specific Threats, Training and Awareness. The Attitudes component assessed Perceived Importance of Cybersecurity and

Confidence in Identifying Security Incidents. The Practices component included questions on the Use of Security Software, Email and Attachment Handling, Device Usage and Data Handling, Software Installation Practices, Computer Locking Practices, and Password Sharing.

A total of 13 items were developed to evaluate these aspects, with each item designed and validated based on existing literature to ensure relevance and clarity. To improve comprehension among participants, the questionnaire was translated from English to Indonesian, addressing potential language barriers. Following data collection, responses were back-translated into English to verify consistency and accuracy.

Data were collected using a self-administered questionnaire distributed to participants in each hospital. Participation in the survey was entirely voluntary and anonymous. Written informed consent was obtained from all participants before completing the questionnaire. Respondents were assured that their responses would remain confidential and would be used solely for research purposes. Descriptive statistics were employed to summarize the frequencies of items related to Knowledge, Attitudes, and Practices (KAP). To identify differences between hospitals, a Chi-Square test was conducted.

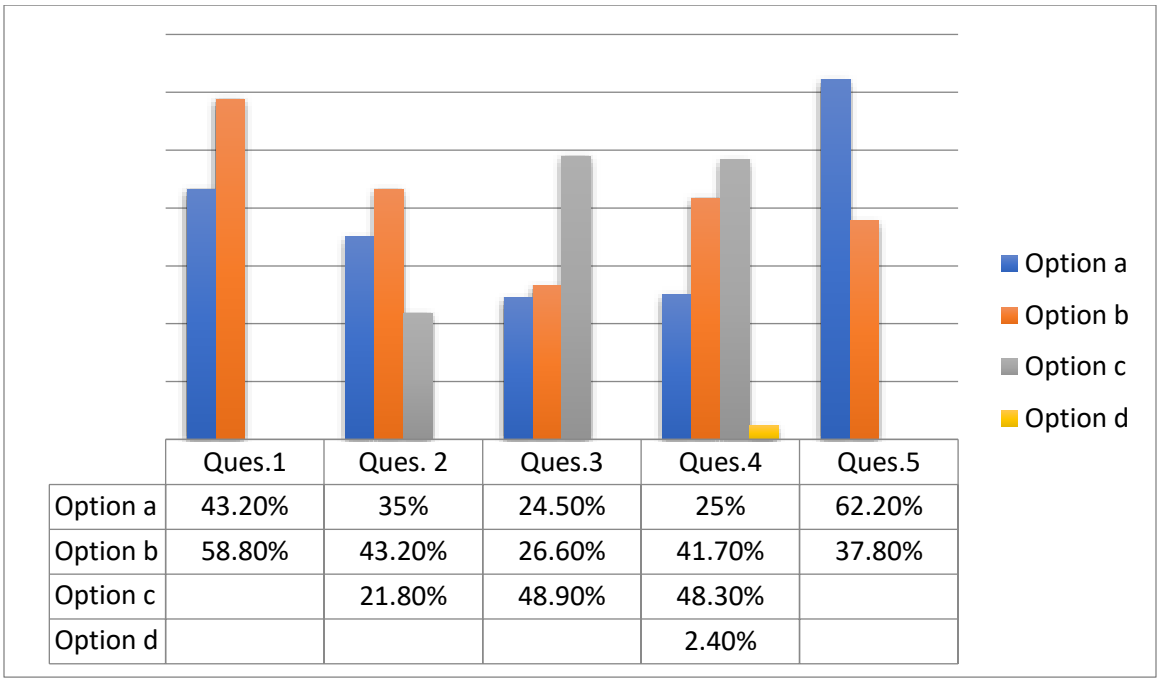
This study obtained approval from the institutional review board of each participating hospital. All procedures were conducted in accordance with ethical standards and guidelines for research involving human participants. Respondents were informed of the study's objectives, assured of their anonymity, and provided written informed consent.

Ethical Approval

Ethical approval for this study was obtained from the Health Research Ethics Committee of Universitas Hasanuddin (979/UN4.14.1/TP.01.02/2024). All key stakeholders signed an informed consent form prior to participating in the study.

RESULTS

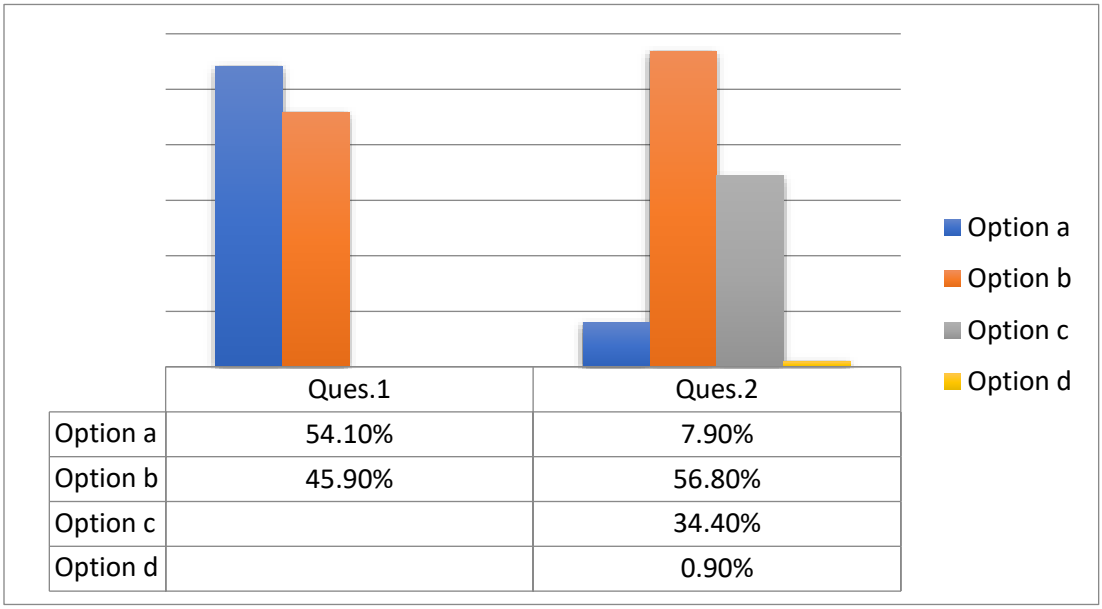
Knowledges



	Ques.1	Ques. 2	Ques.3	Ques.4	Ques.5
Option a	43.20%	35%	24.50%	25%	62.20%
Option b	58.80%	43.20%	26.60%	41.70%	37.80%
Option c		21.80%	48.90%	48.30%	
Option d				2.40%	

From the table above, it is obtained that in question 1 the highest respondent's answer is option b (58.80%), in question 2 the highest answer respondent is option b (43.20%). Then for question 3, the most respondents answered option c (48.90%). Question 4 with the highest respondent answer is option c (48.30%) and the lowest is option d (2.40%). And in question 5 the highest answer is option a (62.20%).

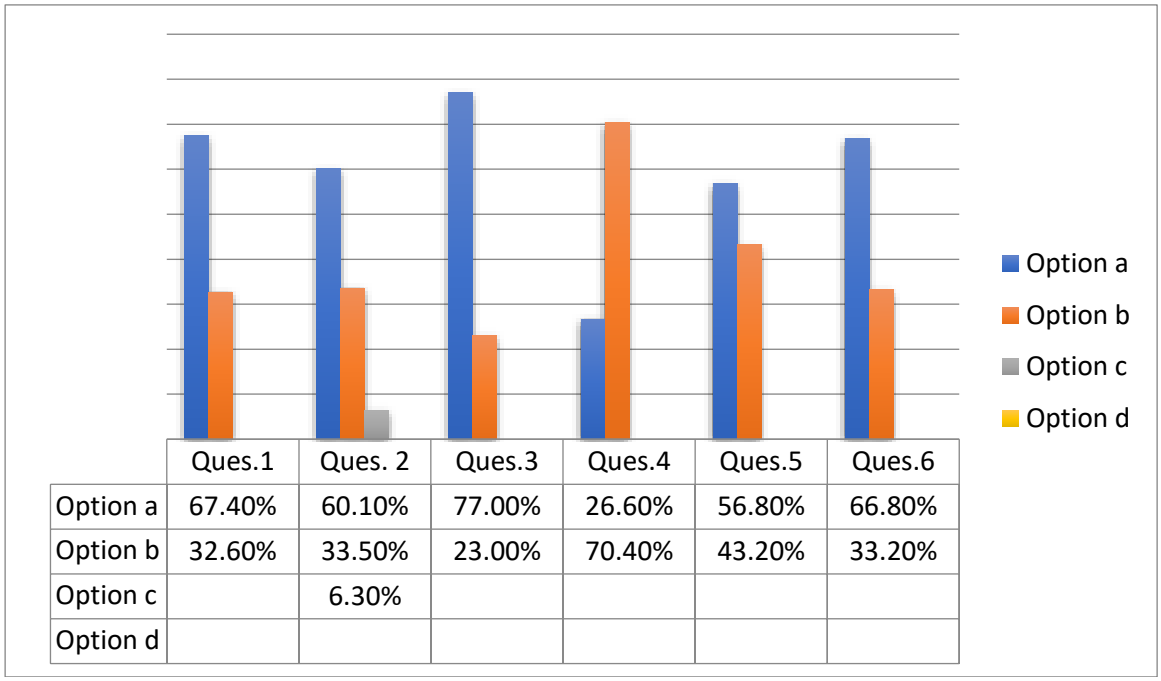
Attitudes



	Ques.1	Ques.2
Option a	54.10%	7.90%
Option b	45.90%	56.80%
Option c		34.40%
Option d		0.90%

From the table above, it is obtained that in question 1 the highest answer is option a, namely (54.10%) and question 2 the highest answer is option b (56.80%).

Practices



	Ques.1	Ques. 2	Ques.3	Ques.4	Ques.5	Ques.6
Option a	67.40%	60.10%	77.00%	26.60%	56.80%	66.80%
Option b	32.60%	33.50%	23.00%	70.40%	43.20%	33.20%
Option c		6.30%				
Option d						

From the table above, it is obtained that in question 1 the highest answer is option a (67.40%), then in question 2 the highest answer is option a (60.10%). In question 3 the highest answer is option a (77.00%), question 4 the highest answer is (70.40%). For question 5, the highest answer is option a (56.80%). And the last one in question 6 is option a (66.80%).

This study assessed cybersecurity knowledge, attitudes, and practices among healthcare workers in three hospitals of varying sizes. A total of 331 healthcare workers participated: 109 from Hospital 1, 139 from Hospital 2, and 83 from Hospital 3. Hospital 2 is the largest, followed by Hospital 1, while Hospital 3 is the smallest.

The study included 331 nurses from three government hospitals in South Sulawesi, Indonesia, offering a representative view of cybersecurity perspectives and practices among nursing staff in provincial hospital settings. For detailed findings on knowledge, attitudes, and practices related to cybersecurity, please refer to Table 1, which presents specific response distributions and insights across these core areas.

Table 1. Summary of Nurses' Knowledge, Attitudes, and Practices Regarding Cybersecurity

No	Questions	Hospital 1 n=109 (100%)	Hospital 2 n=139 (100%)	Hospital 3 n=83 (100%)	*p value*
A.	**Knowledges**				
1	Does the hospital where you work have a hospital cybersecurity policy?				0,03
	a. Yes	35.80%	39.60%	59.00%	
	b. No	64.20%	60.40%	41.00%	
2	Do you know when your computer is hacked or infected and who to contact when that happens?				
	a. Yes, I know when my computer is hacked or infected, and I know whom to contact	23.90%	48.90%	26.50%	0,001
	b. No, I do not know when my computer is hacked or infected, and I do not know whom to contact	40.40%	45.30%	43.40%	
	c. No, I do not know when my computer is hacked or infected, but I know whom to contact	35.80%	5.80%	30.10%	
3	Do you know what email fraud is and how to identify it?				
	a. Yes, I know what email fraud is and how to identify it	8.30%	24.50%	45.80%	
	b. I know what email fraud is but do not know how to identify it	33.00%	17.30%	33.70%	0,001
	c. No, I do not know what email fraud is or how to identify it	58.70%	58.30%	20.50%	
4	I feel adequately trained regarding cybersecurity in the hospital				
	a. Strongly agree	0,10%	9.40%	14.50%	
	b. Agree	43.10%	37.40%	47.00%	0,001
	c. Disagree	55.00%	52.50%	32.50%	
	d. Strongly disagree	1.80%	0.70%	6.00%	
5	Do you know what a social engineering attack is?				
	a. Yes	60.60%	74.80%	43.40%	0,001
	b. No	39.40%	25.20%	56.60%	
B.	**Attitudes**				
6	My computer is of no value to hackers, and hackers are not targeting me				0,635
	a. Yes	56.90%	51.10%	55.40%	
	b. No	43.10%	48.90%	44.60%	

7	I am confident that I can recognize a security problem or incident if I see one				
	a. Strongly agree	0.50%	5.30%	21.70%	0,001
	b. Agree	72.00%	52.20%	42.20%	
	c. Disagree	27.00%	41.00%	32.50%	
	d. Strongly disagree	0.50%	1.50%	3.60%	
C.	**Practices**				
8	Is antivirus software currently installed on your computer?				
	a. Yes	69.70%	66.20%	66.30%	0,815
	b. Know	30.30%	33.80%	33.70%	
9	How cautious are you when opening email attachments?				
	a. I always make sure the email is from someone I know, and I am expecting it	74.30%	48.90%	60.20%	0,002
	b. If I know the person or company sending it, I will open the attachment	20.20%	43.90%	33.70%	
	c. There is no harm in opening attachments	5.50%	7.20%	6.00%	
10	Do you use personal devices, such as mobile phones, flash drives, or CDs/DVDs, to store or transfer confidential hospital information?				0,100
	a. Yes	83.50%	71.90%	77.10%	
	b. No	16.50%	28.10%	22.90%	
11	Do you download and install software on your computer at the hospital?				0,001
	a. Yes	14.70%	30.90%	47.00%	
	b. No	85.30%	69.10%	53.00%	
12	Do you lock your computer when you leave the hospital, even for a moment?				0,772
	a. Yes	54.10%	57.60%	59.00%	
	b. No	45.90%	42.40%	41.00%	
13	Do you give your password to coworkers or your manager when asked?				0,001
	a. Yes	72.50%	77.70%	41.00%	
	b. No	27.50%	22.30%	59.00%	

Knowledge of Cybersecurity

The results revealed significant gaps in cybersecurity knowledge across all hospitals. Only 43.2% of respondents were aware of a hospital cybersecurity policy. Hospital 3 had the highest awareness (59.0%), while Hospitals 1 and 2 reported lower awareness levels (35.8% and 39.6%, respectively) ($p = 0.03$).

Awareness of detecting hacks or infections was similarly low. Across all hospitals, 43.2% of respondents did not know how to recognize a compromised computer or whom to contact. Hospital 2, the largest, had the highest level of awareness (48.9%), while Hospital 1, the second largest, had the lowest (23.9%) ($p = 0.001$). These findings suggest that larger hospitals may face challenges in ensuring uniform knowledge across staff.

Social engineering and email fraud were other areas of concern. While 62.2% of participants recognized the threat of social engineering, only 24.5% could identify email fraud. Hospital 3 had the highest level of awareness

(45.8%), while Hospitals 1 and 2 lagged (p = 0.001). This highlights the need for more focused training on these issues, especially in larger hospitals.

Attitudes toward Cybersecurity

Attitudes towards cybersecurity revealed complacency among healthcare workers. Fifty-four percent of respondents believed their computers were not targeted by hackers. This perception was strongest in Hospital 2 (55.4%), the largest hospital. Despite this, confidence in recognizing security problems was low across all hospitals. Only 7.9% strongly agreed they could identify cybersecurity incidents, with the highest confidence found in Hospital 3 (21.7%) (p = 0.001). This suggests that smaller hospitals may be more effective in fostering vigilance.

Cybersecurity Practices

The survey also examined cybersecurity practices. Although 67.4% of participants had antivirus software installed, 77.0% used personal devices—such as phones and USB drives—to store or transfer confidential hospital data. Hospital 1 had the highest rate of personal device use (83.5%), followed by Hospital 2 (71.9%). These practices pose significant security risks, especially in larger hospitals with complex data management systems.

Despite 56.8% of respondents locking their computers when leaving their workstations, 66.8% admitted to sharing passwords with coworkers or managers. This behaviour was most prevalent in Hospital 2 (77.7%). Password sharing represents a critical vulnerability, especially in larger institutions.

Subgroup Analysis

Subgroup analyses based on hospital size revealed key differences in cybersecurity practices. Hospital 3, despite being the smallest, showed better knowledge and more cautious practices, particularly regarding email fraud and securing computers. In contrast, the larger hospitals, especially Hospital 2, exhibited more complacent attitudes and a higher prevalence of risky practices, such as password sharing and personal device use. These findings highlight the need for tailored interventions based on hospital size. The results suggest significant deficiencies in cybersecurity knowledge and practices across all hospitals. Smaller hospitals, like Hospital 3, may have more effective cybersecurity awareness initiatives, while larger hospitals, like Hospital 2, face challenges related to their size and complexity. The findings emphasize the need for comprehensive cybersecurity training and stronger enforcement of policies, especially in larger hospitals, where organizational structure may hinder consistency in cybersecurity practices.

DISCUSSION

Interpretation of Key Findings

This study reveals significant gaps in cybersecurity knowledge, attitudes, and practices among nurses in Indonesia. Awareness of hospital cybersecurity policies is notably low, which mirrors broader trends in healthcare institutions across Asia. The absence of comprehensive cybersecurity frameworks and awareness programs exacerbates this vulnerability. Many Asian countries, including Indonesia, lag behind Western nations in implementing robust cybersecurity measures, as evidenced by the increasing number of cyberattacks targeting healthcare institutions in the region(15). Human vulnerabilities, such as susceptibility to social engineering attacks, are a major concern. There is a need for increased awareness and training programs to address these issues(16).

The findings show that nurse awareness of hospital cybersecurity policies was low, with only 43.2% of respondents across all hospitals aware of such policies. This was especially evident in Hospitals 1 (35.8%) and 2 (39.6%), the larger institutions, while Hospital 3, the smallest, demonstrated better awareness (59.0%) (p = 0.03). This suggests that smaller, more centralized hospitals may be better equipped to implement focused training programs and maintain consistent cybersecurity awareness across staff. In contrast, larger hospitals may face challenges due to their size and complexity.

Furthermore, awareness of how to recognize computer infections or whom to contact in case of a breach was insufficient. Only 35% of respondents in the largest hospital (Hospital 2) were able to identify cybersecurity threats, indicating a potential gap in internal training and communication, particularly in larger institutions.

The prevalence of risky behaviours, such as the use of personal devices to transfer sensitive hospital data, further highlights the cybersecurity concerns. While 67.4% of participants reported having antivirus software installed, 77.0% admitted using personal devices to store or transfer sensitive data. Hospital 1 had the highest incidence (83.5%), suggesting insufficient data security protocols, particularly in larger hospitals.

Our study contributes to existing research by comparing hospitals of different sizes and identifying key differences in cybersecurity practices. Larger hospitals, while having more resources, face challenges in maintaining consistent cybersecurity practices due to their size. Smaller hospitals, although constrained by resources, benefit from more cohesive organizational cultures that may foster more focused training and policy implementation (17).

Comparison with Previous Studies

Our findings align with prior research indicating insufficient cybersecurity knowledge among healthcare workers. Many healthcare professionals perceive cybersecurity as an IT issue, leading to a lack of engagement with security practices(18). This perception may explain why larger hospitals (Hospitals 1 and 2) exhibit more significant gaps in cybersecurity awareness compared to smaller institutions like Hospital 3. Previous studies suggest that smaller institutions often benefit from simpler organizational structures, leading to more efficient communication and training on cybersecurity (19,20). however, contrasting evidence highlights that larger hospitals, with greater resources, may implement more comprehensive security policies and training programs(17). These discrepancies in our findings likely stem from variations in internal policies, workforce composition, and institutional priorities, warranting further investigation.

Additionally, our findings reveal that Hospital 3 demonstrated notably better recognition of social engineering attacks and email fraud compared to its counterparts. This result may be due to unique training programs or initiatives implemented at the hospital. Previous research supports this hypothesis, emphasizing the importance of several factors in improving cybersecurity skills among nurses. These include integrating cyber hygiene into nursing education(5), using personalized and engaging training methods(21,22), providing continuous professional development opportunities(23,24) and ensuring organizational support and resources(24,25). By addressing these factors, healthcare organizations can better equip their workforce to handle cybersecurity threats, protect patient data, and maintain service integrity.

Enhancing cybersecurity in healthcare requires a balanced approach that includes comprehensive training programs, strategic resource allocation, and optimized budget management. Training and awareness are critical for reducing human vulnerabilities, while strategic investment and budget optimization ensure robust cybersecurity infrastructure. These elements together help healthcare organizations protect sensitive data and maintain service continuity (26,27).

Implications for Health Systems and Policy

The implications of this study for healthcare systems and policies are substantial. The gaps in cybersecurity knowledge and the widespread use of personal devices for transferring sensitive data underscore the need for comprehensive training programs. Targeted interventions are necessary to enhance healthcare workers' understanding of cybersecurity, especially in larger hospitals that may struggle with consistent knowledge dissemination.

Our findings align with global health initiatives, such as the WHO’s Global Strategy on Digital Health, which emphasizes the need for improving data security across healthcare settings. Strengthening cybersecurity policies and improving training programs are essential for protecting sensitive patient data and maintaining public trust in healthcare systems. Hospital administrators should prioritize improving awareness of social engineering attacks, email fraud, and infection detection.

Moreover, hospitals should enforce stricter data security protocols, particularly regarding personal devices. These measures are essential for improving data protection and mitigating the risk of cyberattacks in healthcare settings.

Limitations and Cautions

Despite the valuable insights provided, several limitations of this study should be acknowledged. First, the sample size, though adequate, was limited to only three hospitals, which may affect the generalizability of the

findings. Additionally, the reliance on self-reported surveys introduces the possibility of biases, such as social desirability bias, where participants may report behaviours, they believe to be more acceptable rather than their actual practices.

The study also did not explore the underlying reasons for the low awareness of cybersecurity policies in larger hospitals. Further research should address these limitations by expanding the sample size and including hospitals with different characteristics. Future studies should also employ observational or mixed-methods approaches to provide a more comprehensive understanding of the barriers to effective cybersecurity training in healthcare settings.

Recommendations for Future Research

Future research should address these limitations by expanding the sample size to include diverse hospital types and employing observational or mixed-method approaches. This would provide a more comprehensive understanding of the barriers to effective cybersecurity training in healthcare settings.

Additionally, examining the long-term impact of cybersecurity breaches on patient safety, hospital operations, and clinical outcomes should be a priority. Understanding how security incidents affect patient trust and hospital reputation is crucial for shaping future healthcare policies and improving data security measures.

CONCLUSION

This study provides valuable insights into the cybersecurity knowledge, attitudes, and practices of nurses in Indonesia. Significant gaps were identified, particularly in larger hospitals, where awareness of cybersecurity policies and the ability to detect cyber incidents were lower compared to smaller institutions. Risky behaviours, such as the use of personal devices to store or transfer sensitive data, further highlight the need for stricter policies and targeted training programs.

The findings underscore the importance of strengthening cybersecurity training, especially for nurses who play a critical role in handling sensitive patient data. Hospitals should integrate cybersecurity awareness programs into routine training and enforce hospital-wide security policies. Additionally, hospital leaders should prioritize fostering a culture of cybersecurity awareness and addressing organizational challenges that hinder effective communication and knowledge transfer in larger institutions.

It is also recommended that educational institutions develop specialized curricula to enhance cybersecurity knowledge among healthcare workers. Expanding outreach efforts in healthcare settings, particularly in government hospitals, will be crucial to improving compliance with cybersecurity standards. By addressing these gaps, healthcare systems can better protect sensitive patient data and strengthen resilience against cyber threats.

AUTHOR'S CONTRIBUTION STATEMENT

Author 1 and 2 conceptualized the study and developed the study methodology. Author 1, 2, 3, 4, 5, 6, 7 did the data curation. Author 1 and 7 wrote the manuscript. All authors reviewed and edited the manuscript.

CONFLICTS OF INTEREST

The authors declare no conflicts interests

SOURCE OF FUNDING STATEMENTS

The research was funded by Institute for Research and Community Service, Hasanuddin University. The funder had no role in the study design, data collection and analysis, decision to publish or the preparation of the manuscript.

ACKNOWLEDGMENTS

We would like to acknowledge the following organizations for providing permit to participate in the study: Haji Hospital of South Sulawesi Province, Labuang Baji Hospital of South Sulawesi Province, and Sayang Rakyat Hospital of South Sulawesi Province. The authors would also like to thank the Institute for Research and Community Service, Hasanuddin University for Partnership initiative for this research.

BIBLIOGRAPHY

1. Sabet C, Lin JC, Zhong A, Nguyen D. Cybersecurity in the age of digital pandemics: protecting patient data in low-income and middle-income countries. Lancet Glob Heal [Internet]. 2024 Jun 1 [cited 2024 Oct 28];12(6):e911–2. Available from: http://www.thelancet.com/article/S2214109X24001244/fulltext
2. Sardi A, Rizzi A, Sorano E, Guerrieri A. Cyber Risk in Health Facilities: A Systematic Literature Review. Vol. 12, Sustainability. 2020.
3. Kamerer JL, McDermott D. Cybersecurity: Nurses on the Front Line of Prevention and Education. J Nurs Regul [Internet]. 2020 Jan 1;10(4):48–53. Available from: https://doi.org/10.1016/S2155-8256(20)30014-4
4. Rajamäki J, Rathod P, Kioskli K. Demand Analysis of the Cybersecurity Knowledge Areas and Skills for the Nurses: Preliminary Findings. Eur Conf Cyber Warf Secur [Internet]. 2023 Jun 19 [cited 2024 Nov 10];22(1):711–6. Available from: https://papers.academic-conferences.org/index.php/eccws/article/view/1181
5. Kamerer JL, McDermott DS. Cyber hygiene concepts for nursing education. Nurse Educ Today. 2023 Nov;130:105940.
6. Waddell M. Human factors in cybersecurity: Designing an effective cybersecurity education program for healthcare staff. Healthc Manag forum. 2024 Jan;37(1):13–6.
7. Gioulekas F, Stamatiadis E, Tzikas A, Gounaris K, Georgiadou A, Michalitsi-Psarrou A, et al. A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. Healthc (Basel, Switzerland). 2022 Feb;10(2).
8. World Health Organisation. WHO reports outline responses to cyber-attacks on health care and the rise of disinformation in public health emergencies [Internet]. 2021 [cited 2024 Nov 19]. Available from: https://www.who.int/news/item/06-02-2024-who-reports-outline-responses-to-cyber-attacks-on-health-care-and-the-rise-of-disinformation-in-public-health-emergencies
9. Parsons K, Calic D, Pattinson M, Butavicius M, McCormac A, Zwaans T. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Comput Secur. 2017 May 1;66:40–51.
10. Sari PK. Model Perilaku Keamanan Sistem Informasi Kesehatan dan Implikasinya dalam Pengembangan Roadmap Manajemen Keamanan Informasi pada Fasilitas Pelayanan Kesehatan di Indonesia. Universitas Indonesia; 2023.
11. Egelman S, Peer E. Scaling the security wall : Developing a security behavior intentions scale (SeBIS). Conf Hum Factors Comput Syst - Proc [Internet]. 2015 Apr 18 [cited 2024 Oct 28];2015-April:2873–82. Available from: https://dl.acm.org/doi/10.1145/2702123.2702249
12. Hadlington L. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon. 2017 Jul 1;3(7):e00346.
13. Ifinedo P, Akinnuwesi BA. Employees' non-malicious, counterproductive computer security behaviors (CCSB) in Nigeria and Canada: An empirical and comparative analysis. IEEE Int Conf Adapt Sci Technol ICAST. 2015 Mar 25;2015-January.
14. Hore K, Hoi Tan M, Kehoe A, Beegan A, Mason S, Al Mane N, et al. Cybersecurity and critical care staff: A mixed methods study. Int J Med Inform. 2024 May;185:105412.
15. Kandasamy K, Srinivas S, Achuthan K, Rangan VP. Digital Healthcare - Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations. IEEE Access. 2022;10:12345–64.
16. Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, et al. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Sensors (Basel). 2021 Jul;21(15).
17. Jalali MS, Kaiser JP. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. J Med Internet Res. 2018 May;20(5):e10059.
18. Niki O, Saira G, Arvind S, Mike D. Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that. Digit Heal. 2022;8:20552076221104664.
19. Teymourlouei H, Harris V. Effective Methods to Monitor IT Infrastructure Security for Small Business. In: 2019 International Conference on Computational Science and Computational Intelligence (CSCI). 2019. p. 7–13.
20. Alharbi F, Alsulami M, AL-Solami A, Al-Otaibi Y, Al-Osimi M, Al-Qanor F, et al. The Impact of Cybersecurity Practices on Cyberattack Damage: The Perspective of Small Enterprises in Saudi Arabia. Sensors [Internet]. 2021;21(20). Available from: https://www.mdpi.com/1424-8220/21/20/6901

21. Chowdhury N, Gkioulos V. A personalized learning theory-based cyber-security training exercise. Int J Inf Secur [Internet]. 2023;22(6):1531–46. Available from: https://doi.org/10.1007/s10207-023-00704-z
22. Willing M, Dresen C, Gerlitz E, Haering M, Smith M, Binnewies C, et al. Behavioral responses to a cyber attack in a hospital environment. Sci Rep [Internet]. 2021;11(1):19352. Available from: https://doi.org/10.1038/s41598-021-98576-7
23. Kulju E, Jarva E, Oikarinen A, Hammarén M, Kanste O, Mikkonen K. Educational interventions and their effects on healthcare professionals' digital competence development: A systematic review. Int J Med Inform [Internet]. 2024;185:105396. Available from: https://www.sciencedirect.com/science/article/pii/S1386505624000595
24. Arain MA, Tarraf R, Ahmad A. Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization. J Multidiscip Healthc. 2019;12:73–81.
25. Argyridou E, Nifakos S, Laoudias C, Panda S, Panaousis E, Chandramouli K, et al. Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations: Concept Study. J Med Internet Res. 2023 Jul;25:e41294.
26. Khan, W. (2024). Managing Multimillion-Dollar Security Budgets for Maximum ROI: Insights into Optimizing Resource Allocation to Ensure Cost-Effective Security Solutions. Journal of Engineering and Applied Sciences Technology. https://doi.org/10.47363/jeast/2024(6)e136.
27. Jalali, M., & Kaiser, J. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. Journal of Medical Internet Research, 20. https://doi.org/10.2139/ssrn.3100364.