DOI: http://dx.doi.org/10.26483/ijarcs.v13i4.6835

Volume 13, No. 4, July-August 2022

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

ELEVATING INFORMATION SECURITY PRACTICES WITHIN SUDANESE HEALTHCARE ESTABLISHMENTS' STAFF

Khalid Mohammed Osman Saeed
College of Computer Science and Information Technology
Omdurman Islamic University
Khartoum, Sudan

Abstract: In today's digital era healthcare establishments find information technologies invaluable in daily tasks.
The paper strongly based upon a research that is currently being conducted by the author and according to the results from the research survey only 20% of healthcare establishments in Sudan has security initiatives for their employees and make use of electronic security systems or even physical instruments to protect their assets and patients' information, whilst on the contrary, 80% have no security measures or any security policies. This is due to there is a lack of academic and professional literature about information security management and information security culture. Moreover, as grew to the best knowledge of the author and extracted from the results, healthcare community thought their role is to heal patients and they do not have any responsibility to protect patients' information, whereas they deem such role belong to the computer department, even if, these security breaches computer related (e.g. viruses), or socially motivated (e.g. theft of equipment).
Therefore, the overall aim of this paper is to identify factors that assist the implementation of information security culture and practices within healthcare establishments, and assist when conducting awareness programmers, so it discusses the need to promote information security issues within contemporary Sudanese healthcare establishments and the consequent need for appropriate training and awareness schemes.
In addition, the paper highlights sequence basic elements that healthcare establishments should consider when construct a training and awareness program.

Keywords: information security; healthcare security; information security raising

I. INTRODUCTION

Security has tremendous importance in healthcare information systems, but even as, the need is realized, numerous employees are unfamiliar with even basic notions and procedures. Besides, most healthcare establishments are headed for the use of information technology systems for the most part of their work. Furthermore, the momentous of their information dictates a considerable need for its security and to maintain its confidentiality, integrity and availability. However, it has been confirmed that security can only be maintained if all employees with access privileges know, understand and accept the necessary precautions [1]. Many contravenes are consequence of erroneous behavior by employees who are unconscious about security basics. The provision of security consciousness will make it possible for employees to estimate the security implications of their actions and avoid needless jeopardy's. The majority of information technology employees are now well conscious about necessitate for security, with the extremely publicized incidents of hacking, worms, viruses and helping to highlight harms that may be met without it [2].

So understanding such situations assists to make employees more accepting of the security procedures that may be obligatory imposed on their works. In spite of this, it doesn't mean that they appreciate the linked matters. Whilst, sometimes to all intents and purposes all employees make use of passwords, and a few of them pay right notice to choosing, changing and maintaining the confidentiality of them.

In addition, employees possibly will habitually violate some security policies through what they are thinking in their opinion negligible stuff, such as failing to challenge strangers, sharing passwords with workmates. Whilst both cases may appear somewhat negligible, but they are offer the likelihood for serious security violations. As observed, lack of training and awareness lead to a variety of tribulations as inadequate use of passwords, illegal data modification, hacking attempts and data control dilemmas.

By means of these concerns, it is practical to think about how to elevate security practices in healthcare establishments. As such, sufficient promotion of security through training and awareness programs is considered as a fundamental step.

II. ANALYSIS

In the light of the conclusions extracted from the questionnaire results, the lack of management support and the lack of motivation for security are the main issues that facing Sudanese healthcare establishments to have security initiatives or any security preparation programs. In spite of the mentioned here, out of the 75 of the healthcare establishments in Sudan including hospitals, clinics, and dispensaries there are only 15 of them has security initiatives for their employees and 60 of them have no any security programs or any security policies.

The table I and table II drawn from the questionnaire as a result of the question "Have ever your organization offered a security awareness program?", "Do you think your job responsibilities including securing organizations' data or patients' information?" which that shown the need for security promotion within healthcare establishments employees in Sudan and moreover, the motivation of the author behind making this manuscript.

III. ISSUES IN ELEVATING PREPARATION AND AWARENESS

The below section take into account several essential steps that could be taken to tackle the security elevating requirements within healthcare establishments' employees. This guidance's extract from the training and awareness recommendations mentioned in and produced by Advanced Informatics in Medicine, Secure Environment for Information Systems in MEDicine (AIM SEISMED) volume one and two [3,4].

A. Professional Prepration

No doubt employees knew how to perform their ordinary tasks, but more, they should know their job security issues, and receive instruction on how to perform job related security duties as well. And yet, this should transmit unambiguous announcement of what is expected in respect of security, and it make sure that employees has delivered adequate preparation to obey security requirements included in their agreement of employment. Employees should be conscious that punitive deeds will result from violation security policies and offenders and lawbreaker should be seen to be disciplined in order to dishearten or daunt others.

B. Use of Healthcare Systems and Applications

Employees should receive sufficient preparation for any healthcare establishments systems that they are use, and equally covering general operation and use of security features offered. Additionally, documentation should be accessible when needed for reference to supplement and enhancement the preparation provided.

TABLE I. Have ever your organization offered a security awareness program?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	YES	15	20.0	20.0	20.0
	NO	60	80.0	80.0	100.0
	Total	75	100.0	100.0	

TABLE II. Do you think your job responsibilities including securing organizations' data or patients' information?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	YES	8	10.7	10.7	10.7
	NO	67	89.3	89.3	100.0
	Total	75	100.0	100.0	

C. Healthcare establishment preparation programs

Preparation and awareness programs within healthcare establishments should be performed as a procedure of the induction of new employee and as refresher or reminder for existing ones. These initiatives should be founded on the healthcare establishments' security policies and focus on providing fundamental security awareness concepts (e.g. correct use of passwords, backing up of data, awareness of viruses etc.) for all employees.

More specific preparation may be offered at the department level, these preparations should tailor to the employees' and departments need. In addition, such internal preparations should also underscore the relationship among security and maintaining patients' information safety and confidentiality, and underlining the significance of following the recommendation.

D. Professional preparation courses

Employees such like information technology or security will need specific preparation further than the level mentioned above. Because of the sensitivity of such cases more thorough knowledge is required; moreover the preparation suitability of such courses should be examined. Whereas, if the courses required by numerous employees, the prepared employees may be used as a local source of recommendation within the department or the entire institution.

E. Special purpose awareness

Healthcare employees must be prepared to be capable to manage security issues that arise outside the domain of the standard awareness programs. In numerous situations employees will require to be made conscious of these immediately to ensure that they do not expose security to risk.

Information technology or security employees should make sure that other employees are conscious enough of any particular actions that may influence work or them (e.g. resource unavailability, virus detection, systems' errors detection, applications' updates). The way in which additional awareness is provided may vary relying on the importance of the matter (e.g. threats with immediate effect to security should be coped using employees briefings, while in negligible cases details could be coped using memos or email). In any case it must be ensured that the message is successfully transmitted to every related employee.

F. Preparation responsibilities

A Security officer should be responsible for organizing any firm awareness programs. Accordingly, at the department level, preparation should be conducted by the appropriate qualified internal employee or external instructor. Then, security officer and information technology employees can also offer guidance and assist at this stage. Senior employees should follow security procedures in order to encourage conformity from those at lower levels. However, general employees should also be capable to contact the security officer to set up their preparation needs.

Finally, by following these recommendations, an appropriate training framework may be established.

IV. CONCLUSION

The paper has delineated a sort of variety of ideas that will facilitate a broad methodology to Sudanese healthcare establishments' security awareness to be recognized and established. Nevertheless, it must become conscious that even with these spots took into account the security matter should not be measured completely or absolutely resolved. The preparation agenda and structure must actually be employed and the recommendation it offers should be on a

regular basis reviewed, analyzed and appraised in order to sustain and maintain its relevance.

The authors' now conducting a research study to address security matters on numerous organizations, therefore can be considered to be making importance contribution to the in general security awareness matters within Sudanese organizations.

Nevertheless, again the research dependent on a receptive audience and adherence to the recommendation by the numerous organizations' employees involved.

Consequently, be concluded that in the same way as employees represent the weakest link in the security strategy, they are also the potential weakness of the awareness or preparation program.

V. ACKNOWLEDGMENT

The author's would like to express his gratitude to all the students, colleagues, and employees, for their help have made the successful completion of this manuscript.

VI. REFFRENCES

[1] Viiveke Fak, Amund Hunstad, and E. Graham Dougall (Ed), "Teaching security basics: The importance of when and how", IFIP/Sec '93 Proceedings of the IFIP TC11, Ninth International Conference on Information Security: Computer Security, North-Holland Publishing Co., 1993.

[2] Audit Commission for Local Authorities and the National Health Service in England and Wales (Author), "Opportunity Makes a Thief: An Analysis of Computer Abuse", HMSO Publications Centre, 13 October 1994.

[3] Steven Furnell, Peter Sanders and Matthew Warren, "Baseline Security Guidelines for Health Care Management" in Data Security in Health Care-Volume 1 Management Guidelines, The SEISMED Consortium (Ed), Technology and Informatics 31, IOS Press, 1996.

[4] Steven Furnell, Peter Sanders and Matthew Warren, "Baseline Security Guidelines for Health Care Information Technology and Security Personnel" in Data Security in Health Care-Volume 2 Technical Guidelines, The SEISMED Consortium (Ed), Technology and Informatics 32, IOS Press, 1996.