Public Health and Informatics
J. Mantas et al. (Eds.)

doi:10.3233/SHTI210248

A Simple Assessment of Information Security Awareness in Hospital Staff Across Five Danish Regions

Thomas SCHMIDT[a,1], Christian NØHR[a] and Ross KOPPEL[b,c]
[a] *Center for Health Informatics and Technology, University of Southern Denmark*
[b] *Biomedical Informatics, University of Pennsylvania, Phila., PA, USA*
[c] *Department of Biomedical Informatics University at Buffalo, NY, USA*

Abstract. Information Security Awareness among employees in healthcare has become an essential part in safeguarding health information systems against cyber-attacks and data breaches. We present three simple security awareness questions that can be included in larger surveys gauging other aspects of information systems. The questions have been tested in a national Danish survey to evaluate correlations among medical profession, computer proficiency, experience, and place of employment. We find that dissatisfaction with system usability is strongly linked with reduced information security awareness, and that clinical professions have different responses to security concerns.

Keywords. Computer security, security behaviors, information security awareness

1. Introduction

Information and cyber security are complex disciplines that draw on multiple interconnected concerns ranging from human behaviors, policies, technology, and many other areas. In a context where daily operations depend on a complex interplay of internal and external systems, suppliers, and end-users; public and private institutions are becoming increasingly aware that simple, one-dimensional approaches to improving security, such as only upgrading elements of network security, are insufficient. This is especially apparent in healthcare where any kind of failure can have serious consequences for patients, the organization, as well as staff.

The socio-technical composition of our healthcare systems poses a major challenge for all aspects of security as so many security incidents are either initiated by or directly involve human error. Consequently, addressing security awareness should be a top priority in any organizational effort to improve resilience.

Surveys are frequently used tools for assessing the level of information security awareness. However, due to the cost, concerns about representativeness, and response rates, it is often infeasible to dedicate an entire survey to security concerns. As an alternative to extensive security surveys, we propose a small set of simple information security-related questions for use in larger informatics-related surveys to enable

[1] Thomas Schmidt, Health Informatics and Technology, University of Southern Denmark, Odense, Denmark. E-mail: schmidt@mmmi.sdu.dk

investigators to correlate traits of actual information technology with security awareness. The questions are simplifications of frameworks from the existing literature, and seek to measure aspects of attitude, awareness, and behavior. These aspects have been established as strong tools for assessing information security awareness [1]. The intent of the proposed security awareness instrument is not to provide a full evaluation tool of IT security, but instead for use as a screening tool to determine if further and more elaborate security assessments are needed. The aim of this paper is to present the Simplified Information Security Awareness (SISA) questions and to investigate if there are any associations between clinical profession, employer, or overall satisfaction with current information systems and aspects of information technology security. The SISA questions have been included in a large national survey to Danish healthcare professionals, that represented large areas of Denmark's healthcare systems.

2. Background

Individual characteristics and personality traits of users moderate information security awareness [2], but despite numerous awareness campaigns and prevention mechanisms, human behavior and errors are still the primary points of adversarial approaches to breaching the security of systems [3]. Knowledge of recommended behavior outlined by the organization, commitment, and consequently adherence are typical aspects of information security awareness [1]. These very human characteristics also emphasize that we cannot solely attribute security incidents or data breaches to the malicious intent of adversaries, as incidents often are simply unintended side effects of workarounds. The challenge that good users (accidentally) do bad things has been investigated by experts to highlight the dissonance between assumptions made at a technological managerial level, and work being performed at the operational level [4]. Circumventions often remain hidden until they trigger an unwanted and visible consequence; and with workarounds observed ranging from password management, outbound access, application control, etc. Ensuring security in today's information-driven organizations is not so much a problem of technological character, as it is a matter of understanding human nature [5]. Unsurprisingly, security culture in an organization is strongly linked with information security awareness [6]. Thus, there is ample reason for focusing on how users perceive, relate to, and act upon cybersecurity policies and initiatives. To address this, Parsons et al. developed the Human Aspects of Information Security Questionnaire (HAIS-Q) [1]. Unfortunately, a high level of awareness of risks related to information security is not necessarily associated with behavioral change. However, increased use of technology, which in turn expands exposure to malicious events, is related to a stronger perception of threats [5]. Likewise, certain types of personality traits have been associated with security behaviors, e.g., conscientious students had higher degrees of proactive awareness of information security [7]. As health information systems are deeply ingrained in clinical work, this relationship between perception of system utility and usefulness, and security awareness is of high importance.

3. Methodology

We generalized the HAIS-Q questionnaire by flattening its seven dimensions focusing on the use of computers and data into the three SISA questions that each addressed a

specific aspect of the HAIS-Q. The questions were reviewed by a focus group prior to being tested in the survey. The questions are:

1) **[Awareness]** I am aware of external threats against our data and computers
2) **[Attitude]** I find that the IT-department's initiatives to secure data and computers are more of a nuisance than a benefit
3) **[Behavior]** I am attentive towards how I operate computers to avoid being hacked

Responses are provided using a five-leveled Likert scale. The SISA questions were embedded in a larger national survey on the use of information technology in Danish healthcare. The complete survey included 79 questions and was sent to physicians, nurses, secretaries, and radiographers working in the primary and secondary Danish healthcare sector using the survey tool SurveyXact (www.surveyexact.dk). To ensure response homogeneity, only respondents working at a public hospital will be included in this study. In addition to the SISA questions, we draw upon question from the larger survey which are of relevance to the security awareness aspects and the aim of this paper:

1. **[Complexity]** How many passwords and usernames do you typically use daily?
2. **[IT proficiency]** My colleagues would classify my IT competence level as {ordinary, advanced, expert, don't know}
3. **[System satisfaction]** Overall, how satisfied are you with your EHR system?

Furthermore, the responses include variables such as graduation year (marked as experience), clinical profession, and region of employment. Preprocessing and analysis of responses were conducted in RStudio v.1.2.1x using R v. 3.3. We used Kruskal-Wallis tests to evaluate regional and professional differences by assessing if overall satisfaction with present IT systems varies significantly by profession, region of employment, and level of competence. We combined the awareness, attitude, and behavior responses into a Likert scale, and then applied Dunn tests to assess if parings of professions, and region of employment were statistically significant with regards to SISA responses. The SISA Likert scale also enables us to use ordinal logistic regression to assess the effect of independent parameters.

4. Results

The survey was sent to 9148 professionals. 1621 responded, 1432 of these worked at public hospitals, 1136 responded to the SISA questions, see Table 1. Note that the Danish healthcare system is organized into five regions. The Capital Region (Region C), Region Zeeland (Region Z), Region of Southern Denmark (Region S), Region of Central Denmark (Region M), and Region of Northern Denmark (Region N). Healthcare is one of the key regional responsibilities. Consequently, each region initially deployed five different EHR solutions. However, at the time of this study, Region Z and Region C implemented an EHR system from Epic, Regions S and N rely on systems from foreign vendors, and Region M utilize a platform built in collaboration with a Danish company.

Table 1. Summary of responses

	Physicians n=202 (18%)	**Nurses** n=464 (41%)	**Secretaries** n=379 (33%)	**Radiographers** n=91 (8%)
Region of employment				
Capital Region (32%)	77	137	115	23
Region Zeeland (15%)	38	82	53	12
Region Southern DK (23%)	49	102	84	28
Region Middle DK (20%)	26	102	84	22
Region Northern DK (10%)	12	41	46	6
Level of IT competences				
Expert user	9	34	58	10
Advanced User	61	170	209	49
Regular User	104	225	104	76
Not sure	4	5	8	6
Experience - years (mean-SD)	17.5 - SD 12.1	21.2 - SD 11.7	18.1- SD 11.4	15.1 - SD=12

Differences in system complexity are illustrated by the variances in the daily number of passwords across regions (mean/SD); 1) Region C: 2.6/1.6, 2) Region Z: 2.6/1.8 3) Region S: 3.7/2 4) Region M: 2.2/1.3 5) Region N: 2.7/1.7.

Figure 1 depicts the response distributions for the SISA questions and overall system satisfaction by region. The Dunn test identified two clusters with significant differences in SISA responses, Regions M and N versus Regions C, Z, and S. With regards to differences in professions all group combinations were different, except between radiographers-secretaries. Regression analysis of the SISA scale as outcome with profession, region of employment, level of competence, and overall satisfaction, yielded similar results. I.e., we found that compared to nurses, secretaries and radiographers have a significant positive SISA response, as opposed to physicians who reported significantly fewer concerns about cybersecurity. Regional differences were not significant, neither were competence levels. Experience did significantly positively impact SISA response, and any level above the lowest level of system satisfaction strongly, and significantly, affected security awareness in a positive direction.

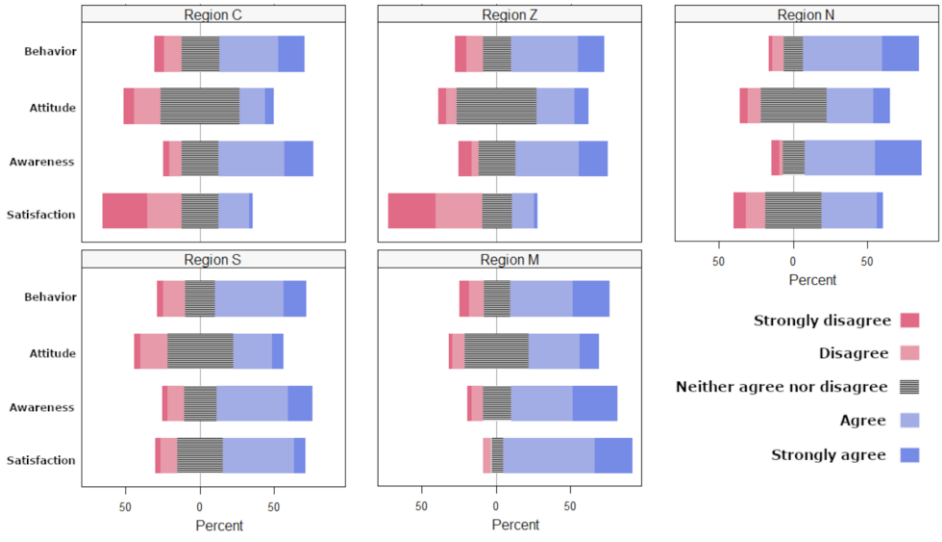

Figure 1. Distribution of responses to the SISA and overall satisfaction questions by region of employment

5. Discussion

Use of EHR's and standardization of work remain an ongoing discussion in Denmark, and we continue to observe substantial regional differences in levels of reported satisfaction with the available IT solutions. Discontent, perceived urgency of tasks, and system friction may increase tendencies to circumvent system safeguards. Although the SISA questions are simple, we see a correlation between satisfaction and information security awareness. In future surveys, we intend to ask the respondents about the frequency of potential circumventions of workflows formalized by information technology. From the responses to the Awareness, Attitude & Behavior questions, it is evident that the Attitude question draws the highest proportion of 'Neither agree nor disagree' responses. This question was negatively phrased - "*I find that the IT-department's initiatives to secure data and computers are more of a nuisance than a benefit*" – and indicate that respondents are either undecided regarding the necessity of imposed security restrictions, or uncertain of the nature of these restrictions. Either way, a challenge remains as how to clarify the importance and impact of behavior constraints.

Using single-item questions to measure a construct is naturally questionable as it is impossible to measure internal consistency. However, certain circumstances, such as restrictions on the number of included questions and survey complexity, suggests the use of single-items is acceptable [8].

6. Conclusion

The results point to a correlation between overall satisfaction with information technology and information security awareness. However, further validation of the SISA questions is needed. We recommend conducting a survey where participants are initially exposed to the SISA, and shortly after the HAIS-Q. This would enable us to use the HAIS-Q responses as a baseline for assessing the validity of the SISA questions.

References

[1] Parsons K, Calic D, Pattinson M, Butavicius M, McCormac A, and Zwaans T, The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies, Comput. Secur. 2017;66:40–51. doi:10.1016/j.cose.2017.01.004.

[2] Mccormac A, Zwaans T, Parsons K, Calic D, Butavicius M, and Pattinson M, Computers in Human Behavior Individual differences and Information Security Awareness, Comput. Human Behav. 2017;69:151–156. doi:10.1016/j.chb.2016.11.065.

[3] Furnell S, and Clarke N, Power to the people ? The evolving recognition of human aspects of security, Comput. Secur. 2012;31:983–988. doi:10.1016/j.cose.2012.08.004.

[4] Blythe J, Koppel R, and Smith SW, Circumvention of Security : Good Users Do Bad Things, IEEE Secur. Priv. 2013;11:80–83. doi:10.1109/MSP.2013.110.

[5] Öǐütçü G, Testik ÖM, and Chouseinoglou O, Analysis of personal information security behavior and awareness, Comput. Secur. 2016;56:83–93. doi:10.1016/j.cose.2015.10.002.

[6] Wiley A, McCormac A, and Calic D, More than the individual: Examining the relationship between culture and Information Security Awareness, Comput. Secur. 2020;88 doi:10.1016/j.cose.2019.101640.

[7] Gratian M, Bandi S, Cukier M, Dykstra J, and Ginther A, Correlating human traits and cyber security behavior intentions, Comput. Secur. 2018;73:345–358. doi:10.1016/j.cose.2017.11.015.

[8] Wanous JP, Reichers AE, and Hudy MJ, Overall Job Satisfaction : How Good Are Single-Item Measures ?, J. Appl. Psycology. 1997;82:247–252.