The Role Of Awareness And Communications In Information Security Management: A Health Care Information Systems Perspective

Sushma Mishra, Robert Morris University, USA
Donald J. Caputo, Robert Morris University, USA
Gregory J. Leone, Robert Morris University, USA
Fred G. Kohun, Robert Morris University, USA
Peter J. Draus, Robert Morris University, USA

ABSTRACT

The purpose and intent of this research study is to understand and interpret the perception of stakeholders in healthcare organizations concerning security awareness and communications. The data is analyzed using the demographic characteristics of age, gender, education, and relevant work experience in order to determine if there are any significant differences between the groups regarding the state of awareness and the communication functions in a health care environment. The statistical results are presented in tabular form with descriptive analysis applied to each of the categories. Data-based conclusions are drawn and future research directions are indicated and discussed.

Keywords: Health Care Information Systems; Security; Privacy; Awareness; Communications; Electronic Medical Records; Compliance

INTRODUCTION

Healthcare information systems are emerging as a major challenge to the security and privacy of electronic health records. Patient health records in electronic form seem to be more susceptible to loss and fabrication issues, thus increasing the security threats to personally identifiable health information. The introduction of the Privacy and Security Rules of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a giant step by the Federal Government to establish some guidelines for patient privacy and security of medical records. Despite strict regulation by governmental agencies such as HIPAA to protect patient information, hospitals are struggling to protect the information of their patients, while security breaches cost the healthcare industry $6 billion annually (Moscaritolo, 2010). A recent survey that defined healthcare records security reveals that the top three causes of breaches were unintentional employee action, lost or stolen computing devices, and third-party accidents. The average number of lost or stolen records per breach was 1,769, with more than 58% of the respondents saying they have "little or no confidence" in their ability to appropriately secure patient records (Moscarito, 2010). Some of these incidents are a direct result of lack of awareness on the part of employees to adequately protect the information, and lack of communication on the part of the management to properly educate employees about the need for strict security measures. A recent survey of privacy and compliance officers at medium-sized hospitals suggests that insiders are responsible for a majority of patient data breaches (eSecurity Planet, 2011). In another incident, a labeling blunder has exposed the private data of nearly 50,000 elderly and vulnerable patients in California. Their social security numbers were inadvertently printed on address labels used in mass mailing (Gonsalves, 2010).

Based on a previous study (Mishra et al., 2011) on the security of healthcare records, this study intends to determine if there is any significant difference in population in its perception about security awareness in employees, and resulting communications efforts by the management. The sample of population that was surveyed for the previous study is also used in this study to determine the stated perceptions based on four criteria: age, gender, education, and years of relevant work experience.

In the context of this study, the following two research questions are used:

RQ1: Is there any difference in the perception of the population regarding security awareness based on age, gender, education level, and professional work experience?

RQ2: Is there any difference in the perception of the population regarding security communications to employees based on age, gender, education level, and professional work experience?

The study uses 9 items to assess security awareness for the population and uses 6 items to assess for security communications. The items are listed below in the results section.

DATA COLLECTION

This is a follow-up study and no new data was collected for the purposes of this study. In the previous study (Mishra et al., 2011), a survey with 43 items was developed and conducted. In this study, the data collected about the demographics of the population is being used to traverse the state of security awareness and communication efforts in this regard. Data was collected using a paper based survey. Masters and doctoral students in the area of nursing in 3 different universities took the survey. There are a total of 64 usable responses. The respondent profile could be described as:

1. All the respondents have work experience in the health care industry and a majority (> 60%) of them had more than one year relevant experience.
2. A majority of the respondents are working in computerized (partially or fully) health care facilities (more than 95%).
3. A majority of the respondents have an undergraduate degree (50%) followed by a Masters degree (41.93%).
4. About 5% of the respondents hold a doctoral or equivalent degree and work primarily in administrative roles in health care organizations. This suggests a mature and educated set of respondents.
5. For gender composition, 62.5% of the respondents were female and 37.5% were male.
6. A majority of the respondents (52.45%) belonged to the age group of 20-30 years followed by (16.39%) each for the age group 31-40 and 41-50 (see Table 4). The remaining respondents belonged to an age group of 50-60 years.

The data from the survey were imported in SPSS for analysis.

RESULTS

Population Characteristics: Age

RQ1: Is there any difference in the perception of the population regarding security awareness based on age, gender, education level, and professional work experience?

The survey questions used to answer RQ1 follows:

Table 1: Research Question 1 with All Items for Each Age Group

Age Groups	All	Mean of Groups			
		20-30 N = 33	**31-40 N = 10**	**41-50 N = 11**	**50-Older N = 10**
16) Security policies and procedures are easily accessible and comprehendible in my organization.	1.95	1.82	2.00	2.00	2.30
18) We emphasize having informal meetings and discussions about the importance of managing security and privacy of the records in my organization.	2.49	2.30	2.80	2.18	1.17
21) Training about security measures is provided regularly to the staff/personnel in my organization.	2.03	1.91	1.70	2.00	2.40
22) In my organization, security policies and procedures are periodically reviewed.	2.15	1.91	1.60	2.36	2.20
24) In my organization, I understand what information I have access to and why?	1.84	1.94	1.70	1.73	1.80
26) I am required to access health information only through approved devices and software in the organization.	1.61	1.64	1.20	1.36	1.90
30) I am allowed to use removable storage media from outside on my machine in the organization.	2.98	3.15	3.00	2.82	2.60
31) In my organization, I am required to obtain permission to use social networking sites.	2.81	2.61	3.50	2.18	2,70
33) I am aware of the procedure about what to do when my system has malware in my organization.	2.57	2.76	2.00	2.18	2.70

Research Question 1 (categorized by age) on this table displays the response to security procedures, training, and education endeavors as perceived by four (4) age groups. The reasonable assumption of managerial status, derived from experience and maturation, is that the older age groups are at the strategic end of the spectrum, and that the younger groups likely are at the operational stage. Detailed procedures are more commonly accepted at the lower age levels, while informal aspects of security are evaluated and accepted by the highest age group as a more seasoned approach to security concerns. Question 16 is an anomaly since the high mean score indicates a negative among the older groups. Given the age of this group it would appear that, due to their experience, they have the best access and knowledge of security policies.

RQ2: Is there any difference in the perception of the population regarding security communications to employees based on age, gender, education level, and professional work experience?

The survey questions used to answer RQ2 follows:

Table 2: Research Question 2 with All Items for Each Age Group

Age Groups	All	Mean of Groups			
		20-30 N = 33	**31-40 N = 10**	**41-50 N = 11**	**51-Older N = 10**
20) Access to the system is based on the role that I play in the organization.	1.68	1.67	1.80	1.46	1.70
23) There exists a clear structure for disciplinary action in case of noncompliance with policies and procedures in my organization.	1.73	1.49	2.10	1.82	1.70
27) I am required to report any misuse of information (that I am in-charge of) or its inappropriate access.	1.60	1.55	1.50	1.36	1.80
28) I am aware of the password policy that I have to comply with, in my organization.	1.55	1.55	1.60	1.27	1.80
29) I frequently receive communication about acceptable security behavior in my organization.	2.15	2.03	2.00	1.55	2.70
34) In my organization, there is an ongoing effort on training and education of employees about security issues.	2.24	2.21	2.10	2.00	2.50

Research Question 5 (categorized by age) on this Table 2 displays a pronounced dichotomy between the Highest (51+) age group and the next highest age group (41-50). The two groups at the lowest age level are indistinguishable in their responses at either end of the scale. The eldest group displays a pronounced lack of agreement within the tenets of the research questions, while the age 41-50 group, only marginally younger, directs their attention to an overwhelming mutually high assessment of strong agreement and compliance at every stage except that of discipline. The higher scores for Questions 29 and 34 were for the oldest group of respondents. The responses to these questions may indicate a 'lack of interest' among these respondents regarding their attitudes shaped by years of pressure pertaining to these HIPPA issues.

Population Characteristics: Year of Work Experience

RQ1: Is there any difference in the perception of the population regarding security awareness based on age, gender, education level, and professional work experience?

The survey questions used to answer RQ1 follows:

Table 3: Research Question 1 with All Items for Work Experience

Years Worked	All		Mean of Groups			
		0 Years N = 24	1-5 Yrs N = 15	6-10 N = 10	11-15 N = 5	More Than 15 N = 9
16) Security policies and procedures are easily accessible and comprehendible in my organization.	1.95	1.88	2.00	1.70	2.20	2.44
18) We emphasize having informal meetings and discussions about importance of managing security and privacy of the records in my organization.	2.49	2.21	2.67	2.70	2.00	2.44
21) Training about security measures is provided regularly to the staff/personnel in my organization.	2.03	2.13	1.73	1.70	2.20	2.33
22) In my organization, security policies and procedures are periodically reviewed.	2.15	1.75	1.73	2.50	2.00	2.67
24) In my organization, I understand what information I have access to and why?	1.89	2.08	1.53	2.10	1.40	1,89
26) I am required to access health information only through approved devices and software in the organization.	1.61	1.79	1.33	1.40	1.60	1.67
30) I am allowed to use removable storage media from outside on my machine in the organization.	2.98	3.13	3.00	3.10	3.20	2.67
31) In my organization, I am required to obtain permission to use social networking sites.	2.81	2.50	3.27	2.30	3.20	2.67
33) I am aware of the procedure about what to do when my system has malware in my organization.	2.57	2.50	2.87	2.40	2.80	2.33

Research Question 1 (categorized by years worked) notes some interesting similarities to the preceding two tables, specifically when examining the low agreement level of the highest age levels and the longest tenure in years of work experience. Thus, a relationship (as predicated earlier) exists between age and years worked, not just in management philosophy, but in procedural policy. Those respondents with less than 1 year of work experience had no significant leanings toward either strong agreement or strong disagreement. Questions 16 and 18 correlate with the negative acceptance of these issues by those who have the most number of years of work experience.

RQ2: Is there any difference in the perception of the population regarding security communications to employees based on age, gender, education level, and professional work experience?

The survey questions used to answer RQ2 follows:

Table 4: Research Question 2 with All Items for Work Experience

Years Worked	All		Mean of Groups			
		0 Years N = 24	1-5 N = 15	6-10 N = 10	11-15 N = 5	More Than 15 N = 9
20) Access to the system is based on the role that I play in the organization.	1.68	1.92	1.33	1.90	1.60	1.44
23) There exists a clear structure for disciplinary action in case of noncompliance with policies and procedures in my organization.	1.73	1.71	1.40	2.30	1.40	1.67
27) I am required to report any misuse of information (that I am in-charge of) or its inappropriate access	1.60	1.54	1.53	1.80	1.60	1.44
28) I am aware of the password policy that I have to comply with in my organization.	1.55	1.75	1.33	1.70	1.60	1.33
29) I frequently receive communications about acceptable security behavior in my organization.	2.15	1.92	1.87	2.70	1.40	2.56
34) In my organization, there is an ongoing effort for training and education of employees about security issues.	2.24	2.17	2.07	2.60	2.40	2.22

Research Question 2 (categorized by years worked) delves into the communication aspects of Health Care organizations. This table shows almost unanimous rigidity throughout the questions as they progress across the experience plateau, changing unevenly from high to low at each years worked stage. Most remarkably, the two most experienced personnel categories show the highest level of agreement, while the less than 1 and 6-10 year group shows the opposite edge with a strong1y disparate message. The 1-5 year category shares a very strong similarity to the most experienced groups in nearly every aspect of the matrix. In all of the questions except Question 29, those with most years worked are more in agreement with the security issues than those with less years tenure.

Population Characteristics: Gender

RQ1: Is there any difference in the perception of the population regarding security awareness based on age, gender, education level, and professional work experience?

The survey questions used to answer RQ1 follows:

Table 5: Research Question 1 with All Items for Gender

Gender	All		
		Male N = 23	Female N = 41
16) Security policies and procedures are easily accessible and comprehendible in my organization.	1.95	2.17	1.83
18) We emphasize having informal meetings and discussions about importance of managing security and privacy of the records in my organization.	2.49	2.13	2.51
21) Training about security measures is provided regularly to the staff/personnel in my organization.	2.03	1.87	2.02
22) In my organization, security policies, and procedures are periodically reviewed.	2.15	1.87	2.05
24) In my organization, I understand what information I have access to and why?	1.89	1.87	1.83
26) I am required to access health information only through approved devices and software in the organization.	1.61	1.52	1.59
30) I am allowed to use removable storage media from outside on my machine in the organization.	2.98	2.61	3.19
31) In my organization, I am required to obtain permission to use social networking sites.	2.81	2.70	2.68
33) I am aware of the procedure about what to do when my system has malware in my organization.	2.57	2.17	2.73

Research Question 1 (categorized by gender) on this table is characterized by the quite small difference in mean scores throughout the question range. The gender differences do display a slight categorical shift toward the stronger agreement over technical issues such as software and hardware by the male component of the study. The female counterpart reiterates a somewhat marginal interest in networking on a social basis, but no single item stands out as an essential difference between the genders. Question 30 is the only outlier in the table, indicating a disagreement among females allowing the use of removable storage media.

RQ2: Is there any difference in the perception of the population regarding security communications to employees based on age, gender, educational level, and professional work experience?

The survey questions used to answer RQ2 follows:

Table 6: Research Question 5 with All Items for Gender

Gender	All		
		Male **N = 23**	**Female** **N = 41**
20) Access to the system is based on the role that I play in the organization.	1.68	1.78	1.59
23) There exists a clear structure for disciplinary action in case of noncompliance with policies and procedures in my organization.	1.73	1.91	1.54
27) I am required to report any misuse of information (that I am in-charge of) or its inappropriate access.	1.60	1.52	1.56
28) I am aware of the password policy that I have to comply with, in my organization.	1.55	1.44	1.61
29) I frequently receive communications about acceptable security behavior in my organization.	2.15	1.70	2.24
34) In my organization, there is an ongoing effort on training and education of employees about security issues.	2.24	1.96	2.34

Research Question 2 (categorized by gender) on Table 6, is difficult to categorize. The most discrete responses of the female contingent focus on their role in the organization whereas the typical male outlook reflects the structural components of the security and behavior of individuals in their responses.

Questions 28 and 29 indicate the highest mean score for female participants. This may indicate a gender bias relating to the communications protocol of the organizations.

Population Characteristics: Education

RQ1: Is there any difference in the perception of the population regarding security awareness based on age, gender, education level, and professional work experience?

The survey questions used to answer RQ1 follows:

Table 7: Research Question 1 with All Items for Education

Education	All	Mean of Groups			
		High School **N = 2**	**UG Deg** **N = 33**	**Masters** **N = 26**	**Doct** **N = 3**
16) Security policies and procedures are easily accessible and comprehendible in my organization.	1.95	2.50	1.84	2.00	2.33
18) We emphasize having informal meetings and discussions about the importance of managing security and privacy of the records in my organization.	2.49	3.00	2.33	2.38	2.17
21) Training about security measures is provided regularly to the staff/personnel in my organization.	2.03	2.00	1.91	1.96	2.66
22) In my organization, security policies and procedures are periodically reviewed.	2.15	1.50	1.93	2.04	2.33
24) In my organization, I understand what information I have access to and why?	1.89	1.00	1.91	1.81	2.00
26) I am required to access health information only through approved devices and software in the organization.	1.61	1.50	1.49	1.69	1.33

Table 7 cont.

30) I am allowed to use removable storage media from outside on my machine in the organization.	2.98	3.50	3.21	2.76	2.00
31) In my organization, I am required to obtain permission to use social networking sites.	2.81	3.50	2.67	2.73	2.00
33) I am aware of the procedure about what to do when my system has malware in my organization.	2.57	2.50	2.70	2.31	2.67

Research Question 1 on Table 7 (categorized by education) is skewed by the lack of subjects in the survey population at the lowest and highest categories of High School and Doctoral Studies. Thus, only undergraduate and masters level data is explored. Although the differences in means on Question 16 through Question 33 were not, in themselves, noticeably large, the matrix clearly showed a stronger agreement component by the undergraduate class in comparison to the graduate collection. Thus, adherence to policies at the masters level was less than that at the undergraduate level. The undergraduate population mean for Question 30 (indicating a negative reaction to the issues of companies allowing employees to use removable storage media on company equipment) was the highest mean score for all questions. This issue also displays a negative disparity for the female population.

In summary, creating awareness about security issues is an important step in an organization's overall security program. Awareness about security vulnerabilities can be effectively created through proper education and training modules in an organization (Dhillon & Torkzadeh, 2006). This makes an employee aware of responsibilities and risks involved in implementing security controls. Training with work related examples would be useful in understanding the depth and reach of the controls. Also, increasing awareness of social engineering issues is an issue that has arisen more recently, and requires more consideration as a potential problem area. Education, it should be noted, can be provided through regular and frequent training sessions. Information security literature has long emphasized training and education as major components for regulatory security programs. Lack of security control awareness is a major obstacle for effective information systems security governance (Johnson, 2006). Proper training and education results in adopting a more congenial mindset and behavior towards security. Management should take progressive measures designed to increase the awareness of the intent and scope of the security controls (Mishra & Dhillon, 2008).

RQ2: Is there any difference in the perception of the population regarding security communications to employees based on age, gender, education level, and professional work experience?

The survey questions used to answer RQ2 follows:

Table 8: Research Question 2 with All Items

Education	All	Mean of Groups			
		High School	**UG Deg**	**Master**	**Doctorate**
		N = 2	**N = 33**	**N = 26**	**N = 3**
20) Access to the system is based on the role that I play in the organization.	1.68	1.00	1.52	1.89	1.67
23) There exists a clear structure for disciplinary action in case of noncompliance with policies and procedures in my organization.	1.73	1.50	1.67	1.65	2.00
27) I am required to report any misuse of information (that I am in-charge of) or its inappropriate access.	1.60	1.00	1.42	1.69	2.00
28) I am aware of the password policy that I have to comply with, in my organization.	1.55	1.00	1.46	1.69	1.67
29) I frequently receive communications about acceptable security behavior in my organization.	2.15	1.50	1.94	2.19	2.33
34) In my organization, there is an ongoing effort for training and education of employees about security issues.	2.24	2.00	2.24	2.12	2.67

Research Question 2 (categorized by education) had an inadequate response of subjects at the High School and Doctorate level, and thus is not included in the matrix. There is a question of procedural detail versus professional responsibility, and a slight deviation of managerial versus operational status, but most of the variance between these groups on all questions is not substantial.

In summary, organizations should encourage communication about control issues among employees. It would be helpful to have a communication policy that results in frequent discussions about security issues. Employees would be better prepared to follow the controls if they are aware of the rationale and value of the controls and the reasons governing organizational actions (Whitman et al., 2001). Communications act as the backbone for a successful security governance program. COBIT identifies the theme, *communicate management aim and direction* (PO6), as an important objective that stresses the importance of ongoing communications policy to articulate the vision and the objectives of security governance programs (Information Technology Governance Institute, 2006). In COSO framework (COSO, 2007), information and communications, the capture and communication of relevant information for integrity of controls is proposed as an objective.

CONCLUSION

The purpose of this study was to examine the perception of the population about security awareness and communications in organizations based on four characteristics of the population: age, gender, work experience, and education. This study uses the primary data collected by a previous study (see Mishra et al., 2011) to analyze if there is any significant difference in perception of security awareness and communications in healthcare organizations, especially in the context of HIPAA compliance. Two research questions are framed to guide the study. For the most part, there seems to be inadequate or not significant differences in the perception of the population about awareness and communication. This could be attributed to low sample size.

There are several studies that could stem from this particular work. We need more data to hypothesize the differences that have been studied here and test the significance statistically. This study assumes that security needs and challenges for healthcare industry would be similar to other industries. Even though conceptually it makes sense that health care organizations would have similar security issues, it requires more study to search out specific security measures that are tailored more toward health care organizations rather than any other specific type of organization. Even though the security requirements are the same, relatively little has been focused on the unique managerial, regulatory, and policy challenges found in healthcare.

AUTHOR INFORMATION

Sushma Mishra is an assistant professor of computer information systems at Robert Morris University, PA. She received her PhD in Information Systems from Virginia Commonwealth University. Dr. Mishra’s primary research interest lies in the area of information security and governance, health informatics, and assurance. She has presented in several international conferences such as AMCIS, IACIS, ECIS, DSI, IRMA, SAIS, and SEDSI. Dr. Mishra has published in journals such as *Communications of Association of Information Systems*, *Issues in information Systems* and has authored several book chapters in information security governance area. E-mail: mishra@rmu.edu

Don Caputo received his Ph.D. in Information and Educational Technology at the University of Pittsburgh. Currently, he is a Computer and Information Systems Professor at Robert Morris University. He previously taught at Penn State University in the Computer Science department with expertise in Computer Languages, and was an Adjunct Professor in the Doctoral Educational Technology program at the University of Pittsburgh. At Robert Morris University, his area of specialization centers on Health Informatics, Medical Programming Languages, and Decision Support Systems. Dr. Caputo has published in numerous professional journals associated with IACIS, ISECON, NEDSI, IBER, and M Computing. E-mail: caputo@rmu.edu (Corresponding author)

Gregory J. Leone’s primary background has been in information technology both as an administrator and as a faculty member at Robert Morris University. He was hired to direct the university’s entry into the information age for administrative and academic computing in the 1970s. His duties consisted of building a staff of qualified professionals, automating all of the administrative computing functions and building a foundation that brought computing into the academic departments. With the directive from top management, the competence of an outstanding IT staff, and the support and feedback from faculty and staff, the university IT infrastructure and resources have grown dramatically. As part of the doctoral faculty and supporting student doctoral research projects his main focus has been IT related. These projects were both quantitative and qualitative and spanned the areas of both hardware and software and the effect of IT in business, health care and education. E-mail: leone@rmu.edu

Fred G. Kohun, Robert Morris University, USA. E-mail: kohun@rmu.edu

Peter Draus earned his doctoral degree in Instructional Design and Technology from the University of Pittsburgh and holds a Master's degree in Information Science. He has many years of experience writing, programming, and developing multimedia based educational materials for a wide variety of presentation environments. Currently an Associate Professor at Robert Morris University in the Information Systems department, he has held a variety of academic administrative positions at different institutions; from Department Chair to Dean of the College for Information Technology. He has been a ranked faculty member since 1995. His funded and unfunded research has focused on technology, interfaces, education and assessment. Currently, he is working on projects measuring the impact of social media and video on student's performance and expectations. E-mail: draus@rmu.edu

REFERENCES

1. COSO (2007). *Putting COSO theory into practice: Tone at the top*. Committee of Sponsoring Organization of the Treadway Commission. Retrieved 10/10/08 from www.coso.org
2. Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information systems security in organizations. *Information Systems Journal, 16*(3), 293-314.
3. eSecurityPlanet (2011). *Majority of healthcare providers hit by security breaches*. Retrieved 10/12/11 from http://www.esecurityplanet.com/network-security/majority-of-healthcare-providers-hit-by-security-breaches.html
4. IT Governance Institute. (2006). *IT control objectives for Sarbanes Oxley: The role of IT in the design and implementation of internal control over financial reporting* (2nd ed.). Rolling Meadows, IL: IT Governance Institute.
5. Gonsalves, A. (2010). Security breach exposes healthcare recipients' data. *InformationWeek.* Retrieved 10/12/11 from http://www.informationweek.com/news/healthcare/security-privacy/222700692
6. Johnson, R., Hoskisson, R., & Hitt, M. (1993). Board of director involvement in restructuring: The effects of board versus managerial controls and characteristics. *Strategic Management Journal, 14*, 33-50.
7. Mishra, S., & Dhillon, G. (2008). *Defining internal control objectives for information systems security: A value focused assessment*. 16th European Conference on Information Systems (ECIS) June 09-11, Galway, Ireland.
8. Mishra, S., Leone, G., Caputo, D., & Calabrisi, R. (2011). Security awareness for healthcare information systems: A HIPAA compliance perspective. *Issues in Information Systems, XII*(1), 224-236.
9. Moscaritolo, A. (2010). *Breaches cost health care industry $6 billion annually*. Retrieved 10/12/11 from http://www.scmagazineus.com/breaches-cost-health-care-industry-6-billion-annually/printarticle/190493/
10. Whitman, M., Townsend, A., & Alberts, R. (2001). Information systems security and the need for policy. In G. Dhillion (ed.), *Information security management: Global challenges in the new millennium* (pp. 9-18). IGI Global.

NOTES