Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2012 Proceedings | Proceedings

The Role of Demographic Characteristics in Health Care Strategic Security Planning

Sushma Mishra
Computer Information Systems, Robert Morris University, Moon Township, PA, United States., mishra@rmu.edu

Gregory Leone
Computer Information Systems, Robert Morris University, Moon Township, PA, United States., leone@rmu.edu

Donald Caputo
Computer Information Systems, Robert Morris University, Moon Township, PA, United States., Caputo@rmu.edu

Robert Calabrisi
Computer Information Systems, Robert Morris University, Moon Township, PA, United States., calabrisi@rmu.edu

Peter Draus
Computer Information Systems, Robert Morris University, Moon Township, PA, United States., draus@rmu.edu

The Role of Demographic Characteristics in Health Care Strategic Security Planning

Sushma Mishra
Robert Morris University
mishra@rmu.edu

Gregory J. Leone
Robert Morris University
leone@rmu.edu

Donald J. Caputo
Robert Morris University
caputo@rmu.edu

Robert R. Calabrisi
Robert Morris University
calabrisi@rmu.edu

Peter Draus
Robert Morris University
draus@rmu.edu

ABSTRACT

The purpose of this paper is to foster understanding of the perception of members in healthcare organizations concerning three specific dimensions in the realm of security: strategic planning for security, proactive initiatives for security controls, and training preparedness for security perspective within the context of HIPAA compliance. The research data was collected using a survey instrument with 43 items of demographic information. The data collected was analyzed using demographic characteristics such as age, gender, education and relevant work experience. The aim of the analysis is to assess whether any significant differences exist between groups regarding the perception of security strategic planning, proactive initiatives and training issues. 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, strategic planning, electronic medical records, compliance, proactive initiatives, training

INTRODUCTION

Healthcare information technology is a profuse and rapidly growing area, and the sensitive nature of the patient clinical data that these evoke make the security of such entities a major strategic issue for the healthcare industry. The computerization of medical records is aimed at reducing the cost of care and improving patient safety (Samy et al 2010). Threats to health information security have increased over the years with several reported security breaches in media regarding exposure of privileged health information. Storing health care data in electronic format raises concerns about the privacy of patient identity. In-depth studies show that healthcare information systems (HIS) are threatened by both accidental events and deliberate action threats, which can severely damage the health information systems reliability and consequently discourage professionals from future use (Samy et al, 2010). 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.

To create an adequate level of information security for health care information systems, formal information security programs need to be created. To provide comprehensive security programs in an organization, it is very important to strategically plan for security, take proactive security initiatives in the organization and establish proper security training channels in an organization. It is the role of the upper management to entail a security strategy for the entire health care organization

including the care delivery systems. People in higher management such as CIOs or CSOs are typically responsible for creating a vision for the organization. A formal security program needs to be in place for the organization, taking into account various types of threats involved within and outside the network of the health care system.

This study attempts to understand perception of health care service providers in terms of strategic planning for security, formal level management of security initiatives, and security training related issues for successfully protecting health care data from insider and outsider threats. This study intends to determine if there is any significant difference in population in its perception about security strategy in employees, proactive security management and security training procedures for proper computer usage. The sample of population that was surveyed 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 three research questions are used:

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

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

RQ3: Is there any difference in the perception of the population regarding security training procedures for proper computer usage based on age, gender, education level and professional work experience?

The study uses 6 items to assess security strategy and compliance, 8 items for research question 2, which is proactive management and 5 items for research question 3, training for computer usage. The items are listed below in the results section.

DATA COLLECTION AND ANALYSIS

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. For the purpose of this study, the data collected about the demographics of the population is being used to traverse the perception of stakeholders about security strategic planning, proactive initiatives and specific security training modules, especially in the context of HIPAA compliance. Data was collected using a paper-based survey. Masters and doctoral students in the area of nursing in 3 different universities completed the survey. There are a total 64 usable responses. The respondent profile could be described as: all the respondents have work experience in the health care industry and a majority (>60%) of them had more than one year of relevant experience. A majority of the respondents are working in computerized (partially or fully) health care facilities totaling more than 95%). A majority of the respondents have an undergraduate degree (50%) followed by a Masters degree (41.93 %). 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. For gender composition, 62.5 % of the respondents were female and 37.5% were male. 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. The survey items required respondents to rate their response on a scale of 1-5 where 1=strongly agree to 5=strongly disagree. In this context, a low score from the respondent mean higher agreement with the security item.

Results

RQ1: Is there any difference in the perception of the population regarding strategic planning for security from HIPAA compliance perspective based on age, gender, education level and professional work experience? The survey questions used to answer RQ1 are as follows:

Research Question 1 Education	All	Means by Group			
		High School N=2	UG Deg N=33	Masters N=26	Doctoral N=3
1) In my organization, there is a predefined agreed upon plan for security and privacy compliance efforts	1.41	1.50	1.56	**1.23**	1.33
2) There is a prevalent security culture where individuals look out for each other in my organization	2.06	2.00	2.16	**1.84**	3.00
3) Creating security awareness is an ongoing process in my organization	1.88	2.00	**1.84**	1.88	2.33
4) There is visible leadership about the seriousness of security assurance efforts in my organization	1.85	2.00	1.87	**1.81**	2.00
5) In my organization, there are adequate internal controls (policies, procedures, training, encryption, access restrictions) to provide security and privacy of health records	1.69	2.00	**1.61**	1.77	1.67
6) Auditing is viewed as a necessary complimentary action to improve the security initiatives in my organization.	1.91	**1.00**	1.97	1.92	1.67

Table 1: Research question 1 with all items for education level of respondents

Research Question 1 Years worked	All	Means by Group				
		0 yrs	1-5	6-10	11-15	>15
1) In my organization, there is a predefined agreed upon plan for security and privacy compliance efforts	1.41	1.65	1.40	1.20	**1.20**	1.22
2) There is a prevalent security culture where individuals look out for each other in my organization	2.06	2.35	1.93	1.80	**1.80**	2.00
3) Creating security awareness is an ongoing process in my organization	1.88	1.91	1.93	1.80	2.00	**1.78**
4) There is visible leadership about the seriousness of security assurance efforts in my organization	1.85	2.09	1.73	1.70	**1.60**	1.78
5) In my organization, there are adequate internal controls (policies, procedures, training, encryption, access restrictions) to provide security and privacy of health records	1.69	1.91	**1.40**	1.70	1.60	1.67
6) Auditing is viewed as a necessary complimentary action to improve the security initiatives in my organization.	1.91	2.00	1.93	1.80	**1.80**	2.00

Table 2: Research question 1 with all items for years of work experience for respondents

Research Question 1 Ages	All	Means by Group			
		20-30	31-40	41-50	51-older
1) In my organization, there is a predefined agreed upon plan for security and privacy compliance efforts	1.41	1.56	1.30	1.36	**1.10**
2) There is a prevalent security culture where individuals look out for each other in my organization	2.06	2.19	1.90	2.18	**1.67**
3) Creating security awareness is an ongoing process in my organization	1.88	1.94	1.78	2.27	**1.40**
4) There is visible leadership about the seriousness of security assurance efforts in my organization	1.85	2.06	**1.50**	1.82	1.60
5) In my organization, there are adequate internal controls (policies, procedures, training, encryption, access restrictions) to provide security and privacy of health records	1.69	1.71	1.70	2.00	**1.30**
6) Auditing is viewed as a necessary complimentary action to improve the security initiatives in my organization.	1.91	1.90	2.00	2.10	**1.70**

Table 3: Research question 1 with all items for age groups of respondents

Research Question 1 Gender	All	Male N-21	Female N=41
7) Security policies and procedures are easily accessible and comprehendible in my organization	1.95	2.13	**1.85**
8) In my organization, there is an emphasis on establishing open communication channel about security issues without the fear of reprisal.	2.06	2.17	**2.00**
9) We emphasize having informal meetings and discussions about importance of managing security and privacy of the records in my organization	2.49	**2.36**	2.56
10) In my organization, security controls (encryption, access control, password policy, segregation of duty) are viewed as necessary components for security	1.44	**1.43**	1.45
11) Access to the system is based on the role that I play in the organization	1.68	1.65	1.70
12) Training about security measures is provided regularly to the staff/personnel in my organization.	2.03	2.09	2.00
13)In my organization, security policies and procedures are periodically reviewed to assess if the policies meet the changing organizational needs.	2.15	2.09	2.19
14) There exists a clear structure for disciplinary action in case of noncompliance with policies and procedures in my organization.	1.72	1.83	1.67

Table 4: Research question 1 with all items for gender of respondents

For the results of our first research question, on the education level dimension of the respondents, we found that respondents with master's degrees identified the most with questions regarding strategic planning of security for health care organizations. Respondents with master's level education consistently got the lowest mean for three out of 6 items. This result seems to be consistent with the type of roles these respondents with a master's degree have in their organizations in healthcare settings. Most of the respondents with master's degree are in administrative roles and associated with planning health care IT.

Again, the group of people with 11-15 years of work experience seems to have scored the lowest means on all the items that measure the degree of strategic planning of security with health care systems. For the age dimension, people in the age group of 51 or older could relate more to the questions about the strategic dimension of security. This result makes intuitive sense, considering that these are older people who have more administrative knowledge and roles in the organization and who are thus better equipped to understand some of these concerns. Gender wise, females have been more consistent with low scores on most of the items than males, suggesting that they are more concerned about strategic security issues as a group than males.

RQ2: Is there any difference in the perception of the population regarding planning proactive initiatives for HIPAA compliance based on age, gender, education level and professional work experience?

The survey questions used to answer RQ2 are as follows:

Research Question 2 Education	All	Means by Group			
		High School	UG Deg	Masters	Doctoral
7) Security policies and procedures are easily accessible and comprehendible in my organization	1.95	2.00	**1.85**	2.08	2.00
8) In my organization, there is an emphasis on establishing open communication channels about security issues without the fear of reprisal.	2.06	2.00	2.06	**2.04**	2.33
9) We emphasize having informal meetings and discussions about the importance of managing security and privacy of the records in my organization	2.49	2.50	2.45	2.56	**2.33**
10) In my organization, security controls (encryption, access control, password policy, segregation of duty) are viewed as necessary components for security	1.44	2.50	1.45	**1.32**	1.67
11) Access to the system is based on the role that I play in the organization	1.68	2.00	1.75	1.62	**1.33**
12) Training about security measures is provided regularly to the staff/personnel in my organization.	2.03	2.00	2.10	**1.96**	2.00
13) In my organization, security policies and procedures are periodically reviewed to assess if the policies meet the changing organizational needs.	2.15	**1.00**	2.10	2.27	2.00
14) There exists a clear structure for disciplinary action in case of noncompliance with policies and procedures in my organization.	1.72	2.00	1.71	1.73	**1.67**

Table 5: Research question 2 with all items for the education level of respondents

Research Question 2 Years worked	All	Means by Group				
		<1	1-5	6-10	11-15	>15
7) Security policies and procedures are easily accessible and comprehendible in my organization	1.95	2.04	1.87	**1.50**	2.00	2.33
8) In my organization, there is an emphasis on establishing open communication channesl about security issues without the fear of reprisal.	2.06	2.17	2.20	**1.60**	2.00	2.11
9) We emphasize having informal meetings and discussions about importance of managing security and privacy of the records in my organization	2.49	2.57	2.47	**2.33**	3.00	2.25
10) In my organization, security controls (encryption, access control, password policy, segregation of duty) are viewed as necessary components for security	1.44	1.58	1.43	1.30	**1.00**	1.44
11) Access to the system is based on the role that I play in the organization	1.68	2.00	1.73	1.30	**1.20**	1.44
12) Training about security measures is provided regularly to the staff/personnel in my organization.	2.01	2.09	2.20	**1.50**	2.00	2.00
13) In my organization, security policies and procedures are periodically reviewed to assess if the policies meet the changing organizational needs.	2.15	2.24	2.27	**1.56**	2.20	2.13
14) There exists a clear structure for disciplinary action in case of noncompliance with policies and procedures in my organization.	1.72	1.73	2.07	1.60	**1.20**	1.67

Table 6: Research question 2 with all items for years of relevant experiences of respondents

Research Question 2 Ages	All	Means by Group			
		20-30	31-40	41-50	51-older
7) Security policies and procedures are easily accessible and comprehendible in my organization	1.95	2.00	**1.40**	2.45	1.80
8) In my organization, there is an emphasis on establishing open communication channels about security issues without the fear of reprisal.	2.06	2.09	2.00	2.27	**1.80**
9) We emphasize having informal meetings and discussions about importance of managing security and privacy of the records in my organization	2.49	2.50	2.40	3.00	**2.00**
10) In my organization, security controls (encryption, access control, password policy, segregation of duty) are viewed as necessary components for security	1.44	1.53	1.20	1.73	**1.10**
11) Access to the system is based on the role that I play in the organization	1.68	1.97	1.40	1.45	**1.30**
12) Training about security measures is provided regularly to	2.03	2.00	1**.70**	2.36	2.10

the staff/personnel in my organization.					
13) In my organization, security policies and procedures are periodically reviewed to assess if the policies meet the changing organizational needs.	2.15	2.10	2.10	2.67	**1.90**
14)There exists a clear structure for disciplinary action in case of noncompliance with policies and procedures in my organization.	1.72	1.94	1.50	1.82	**1.20**

Table 7: Research question 2 with all items for age group of respondents

Research Question 2 Gender	All	Male N-21	Female N=41
7) Security policies and procedures are easily accessible and comprehendible in my organization	1.95	2.13	**1.85**
8) In my organization, there is an emphasis on establishing open communication channels about security issues without the fear of reprisal.	2.06	2.17	**2.00**
9) We emphasize having informal meetings and discussions about importance of managing security and privacy of the records in my organization	2.49	2.36	2.56
10) In my organization, security controls (encryption, access control, password policy, segregation of duty) are viewed as necessary components for security	1.44	1.43	1.45
11) Access to the system is based on the role that I play in the organization	1.68	1.65	1.70
12) Training about security measures is provided regularly to the staff/personnel in my organization.	2.03	2.09	**2.00**
13) In my organization, security policies and procedures are periodically reviewed to assess if the policies meet the changing organizational needs.	2.15	2.09	2.19
14) There exists a clear structure for disciplinary action in case of noncompliance with policies and procedures in my organization.	1.72	1.83	**1.67**

Table 8: Research question 2 with all items for gender group of respondents

Our second research question is about mid-managerial level concerns of planning for security initiatives proactively in a way that processes are followed and procedures are being well managed. This question was analyzed in this paper based on four demographic dimensions: education level, age, gender and age group. Our results suggest that on an education level dimension, respondents with masters and doctoral level identified more with this mid-managerial level concerns. This could be attributed to the kind of work or roles they have been assigned to in their job environment. On the dimension of years of experiences, the lowest mean is shared between groups with 6-10 years of experience, and the group between 11-15 years of experiences. It is worth noting here that people with experience of 15 years or more do not have the lowest mean. One possible reason for this could be that more work experience could lead to higher positions in the organization pushing these individuals in the realms of strategic planning more than mid-managerial concerns. On the dimension of age group, the respondent in the range of 51 year or older have clearly scored the lowest means. This suggests that the respondents with certain age groups are dealing with security management issues due to job responsibility. Based on gender, there is no clear trend for one particular gender outperforming the other.

RQ3: Are there training procedures for proper computer use relating to information security?

Research Question Three Education	All	Mean of Groups			
		High School	UG Deg	Masters	Doctoral
15) Auditing is viewed as a necessary complimentary action to improve the security initiatives in my organization.	1.84	**1.00**	1.97	1.92	1.67
17) In my organization, there is an emphasis on establishing open communication channels about security issues without the fear of reprisal	1.61	**1.12**	2.06	2.04	2.33
19) In my organization, security controls (encryption, access control, password policy, segregation of duty) are viewed as a necessary component for security	1.54	2.50	1.45	**1.32**	1.67
1.25) I am required to read the security policies frequently (Quarterly, bi annually, annually) in my organization	2.23	2.50	2.43	**2.04**	2.33
32) In my organization, I have frequent communication about social engineering issues and am aware of how such tactics can create vulnerability for our system.	1.34	2.50	2.74	2.50	2.33

Table 9: Research question 3 with all items for educational level of respondents

Research Question Three Years worked	All	Means by Group				
		<1	1-5	6-10	11-15	>15
15) Auditing is viewed as a necessary complimentary action to improve the security initiatives in my organization.	1.84	2.00	1.93	**1.80**	**1.80**	2.00
17) In my organization, there is an emphasis on establishing open communication channels about security issues without the fear of reprisal	1.61	2.17	2.20	**1.60**	2.00	2.11
19) In my organization, security controls (encryption, access control, password policy, segregation of duty) are viewed as a necessary component for security	1.54	1.58	1.43	**1.30**	1.00	1.44
25) I am required to read the security policies frequently (Quarterly, bi annually, annually) in my organization	2.23	2.20	2.67	**1.90**	2.20	2.22
32) In my organization, I have frequent communication about social engineering issues and am aware of how such tactics can create vulnerability for our system.	1.34	2.70	2.64	2.50	3.00	**2.33**

Table 10: Research question 3 with all items for years of relevant experience of respondents

Research Question Three Ages	All	Mean of Groups			
		20-30	31-40	41-50	51-older
15) Auditing is viewed as a necessary complimentary action to improve the security initiatives in my organization.	1.84	1.90	2.00	2.10	**1.70**
17) In my organization, there is an emphasis on establishing open communication channels about security issues without the fear of reprisal	1.61	2.09	2.00	2.27	**1.40**
19) In my organization, security controls (encryption, access control, password policy, segregation of duty) are viewed as a necessary component for security	1.54	1.53	1.20	1.73	**1.10**
25) I am required to read the security policies frequently (Quarterly, bi annually, annually) in my organization	2.23	**2.17**	2.60	2.30	2.20

Table 11: Research question 3 with all items for age groups of respondents

Research Question Three Gender	All	Male N-21	Female N=41
15) Auditing is viewed as a necessary complimentary action to improve the security initiatives in my organization.	1.84	2.05	**1.85**
17) In my organization, there is an emphasis on establishing open communication channels about security issues without the fear of reprisal	2.10	2.17	2.00
19) In my organization, security controls (encryption, access control, password policy, segregation of duty) are viewed as necessary components for security	1.44	1.43	1.45
1.25) I am required to read the security policies frequently (Quarterly, bi annually, annually) in my organization	2.23	2.38	2.21
32) In my organization, I have frequent communication about social engineering issues and am aware of how such tactics can create vulnerability for our system.	2.34	2.70	2.56

Table 12: Research question 3 with all items for gender groups of respondents

Our third research question concerns training for job related computer usage for adequate security, and determining if there is any significant difference between groups based on the demographic dimensions such as age, experience, education level and gender. On the dimension of educational level, we found that people, with lowest education level (high school) did score the lowest mean on training. It is apparent that people in lower level operational positions with non-administrative positions do get the maximum training and understand the importance of it more than others on a higher level. On the dimension of years of experience, clearly the group with the lowest means is the one with experience of 6-10 years. It is intriguing to see how people with more than 6 years of working in an area could be ready to move up in an administrative position and understand the importance of training issues to move ahead in an organization. On the dimension of ages, we found that people in the age group of 51 plus have done very well on these items with a low mean score. This tells us that people who are old enough to have been trained several times or are in administrative ranks and understand the importance of training. Finally, the last dimension gender clearly denotes that females have done better on the training issues than males in the groups.

DISCUSSION

The results from this study present some interesting insights into the security management issues in the health care industry. From the strategic preparation for security management perspective, our results suggest that administrators or top-level

management people in the healthcare industry seem to have identified more with the planning and creating security template for the organization. The typical profile of respondents scoring the lowest means on a majority of items is: people with masters or higher degrees with more than 11 years of experience, and the age group of 50 plus. This description suggests the role of these respondents to be more in administrative top level positions. People in administrative roles typically are involved with planning security strategy and defining enterprise security controls (Dhillon and Torkzadeh, 2006; Johnsson et al, 1993).

The second research question is about security management practices and how can these practices be proactively designed and managed. The profile of the group of respondents who have consistently scored the lowest means here is: people with 6-10 years of work experiences, with undergraduate or master's degree and in the age group of 31-40 or 51 plus. This profile is consistent with what we would expect of people in mid-managerial levels executing the duties of a divisional head or functional head. The issues that this particular group of people identified with are more management and process oriented (Mishra and Dhillon, 2008; ITGI, 2006) rather than strategic, and is consistent with the type of roles they might have in these organizations. For regulatory compliance purposes, operational level workers get more extensive training than people higher up in management, just to understand the requirements to be compliant (Kwon and Johnson, 2011; Whitman et al, 2001).

Our third research question is about training issues and it falls under the realm of operational issues. The group of respondents who identified the most with this set of issues is: people with high school degrees, in the age group of 20-30 or 51 plus and with years of experience between 6-10 years. This group of respondents is comprised of relative new comers to this area of health care IT and are in operational roles where they can understand the need for training more than others and likely receive more training than others groups do.

Contribution

Our analysis suggests that security preparedness and initiatives, even though designed for the entire organization, align with people based on their current role in the organization. People in top management align with planning process, people in mid managerial levels align with management of process, and operational level people align more with training issues to get the day-to-day job done properly. This is the unique contribution of this paper. It would of measurable value to further develop this work and check for this relationship from different stakeholder in the health care setting.

CONCLUSION

The purpose of this study was to examine the perception of the population about strategic security planning, proactive security management initiatives and security training issues in organizations based on four characteristics of the population: age, gender, work experience and education level. Based on the data collected by a previous study (see Mishra et al, 2011), we analyze if there is any significant difference in perception of security planning, proactive management and training within healthcare organizations. Three research questions are framed to guide the study. For the most part, there is a group structure emerging from the data that suggests that people identify with security initiatives based on their roles. But more data would be required to assess whether this relationship will hold true.

There are several studies that could stem from this particular work. We need more data to hypothesize the differences in group perception that have been studied here and test the significance statistically. This study assumes that security needs and challenges for the 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.

REFERENCES

1. COSO (2007)"Putting COSO theory into Practice: Tone at the Top," Committee of Sponsoring Organization of the Treadway Commission Retrieved on 10/10/08 www.coso.org
2. Dhillon, G., and Torkzadeh, G. "Value-focused Assessment of information systems security in organizations," *Information Systems Journal* (16:3) 2006, pp 293-314
3. eSecurityPlanet (2011) Majority of Healthcare Providers Hit by Security Breaches, Retrieved on 10/12/11 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 Edition, Rolling Meadows, IL: IT Governance Institute.
5. Gonsalves, A. (2010) Security Breach Exposes Healthcare Recipients' Data, *InformationWeek,* retrieved on 10/12/11
6. http://www.informationweek.com/news/healthcare/security-privacy/222700692
7. Johnson, R., Hoskisson, R. and Hitt, M. (1993) " Board of director involvement in restructuring: The effects of board versus managerial controls and characteristics " Strategic Management Journal (14), pp 33-50.
8. Kwon, J. and Johnson, M. (2011) The Impact of Security Practices on Regulatory Compliance and Security Performance, Proceedings of *Thirty Second International Conference on Information Systems, Shanghai 2011*
9. Mishra, S. and 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
10. Mishra, S., Leone, G., Caputo, D. and Calabrisi, R. (2011) Security Awareness For Healthcare Information Systems: A HIPAA Compliance Perspective, Issues in Information Systems, Volume XII, No. 1, pp. 224-236, 2011
11. Moscaritolo, A. (2010) Breaches cost health care industry $6 billion annually, Retrieved on 10/12/11 http://www.scmagazineus.com/breaches-cost-health-care-industry-6-billion-annually/printarticle/190493/
12. Samy, G., Ahmadm R. and Ismail, Z. (2010). Security threats categories in healthcare information systems, Health Informatics Journal, 16: 201
13. Whitman, M., Townsend, A., and Alberts, R. "Information Systems Security and the Need for Policy," in: Information Security Management: Global Challenges in the New Millennium., G. Dhillion (ed.), IGI Global, 2001, pp. 9-18.