Key Factors in the Success of an Organization’s Information Security Culture: A Quantitative Study and Analysis

Abstract

This research study reviewed relative literature on information security and information security culture within organizations to determine what factors potentially assist an organization in implementing, integrating, and maintaining a successful organizational information security culture. Based on this review of literature, five factors were determined to potentially contribute to a successful information security culture. A survey instrument was designed to determine if each of the factors had a significant association with a successful organizational information security culture, if the factors had a positive or negative relationship with a successful information security culture, and the strength of the relationship to a successful organizational security culture. The data from 200 useable surveys were analyzed using the Chi Square Test of Independence and Bivariate correlation to determine the relation between each of the factors, the independent variables, and the dependent variable, defined as a successful organizational information security culture. The analysis of this data is presented for both scholarly and practitioner information and use.

Introduction

Securing information within organizations is extremely important, as organizations depend more heavily on information systems to conduct business. Research indicates that information security is increasing in importance due to a variety of both internal and external threats [10]. Additionally, governance and regulations such as the Sarbanes-Oxley Act (SOX) of 2002, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the American Recovery and Reinvestment Act (ARRA) of 2009, and Basel II, which regulates the international banking industry, have placed new requirements on businesses to secure information and meet specific process requirements. Originally, organizations depended on technical controls (hardware and software techniques) to safeguard their information. Over time, organizational information security policies, employee user agreements, personnel security training, and standard operating procedures were developed to improve information security and to incorporate information security into the organizational culture. However, in today’s information risk environment, technical controls, policies, and procedures alone are not sufficient - a more holistic approach is needed to properly secure information.

A holistic approach needs to be taken with information security [6]. It needs to be woven into the very fabric of the organization and should be as much a part of the business as financial accounting or other business functions or processes. Information security must be a part of the overall organizational culture. An organizational culture can be defined as a set of values, beliefs, and behavior patterns that mold the core identity of organizations and helps employees and assist in shaping their behavior [4,5]. Research has indicated that there is a correlation between an organization’s culture, the commitment of its employees, and the organization’s performance [11]. This implied that organizational culture and the commitment of an organization’s employees shape the way the organization performs. Additional research stated that a portion of an organization’s information security culture is based on two dimensions of employees, their knowledge and behavior [15]. The publication stated that in order to ensure successful protection of information assets, organizations need to take a formal approach to establish and maintain an information security corporate sub-culture. Other research show organizations need to emphasize an information security culture by making security a part of their employees’ everyday work routine [18]. This research also stated that this is required to have a successful information security culture. Just as finance, accounting, human resources, and customer relations are part of businesses’ culture, so is information security.

Information Security is a concern of businesses today. Much research has emphasized specific areas that companies need to focus on in order to improve their information security. A problem is that organizations find it difficult to successfully implement, integrate, and maintain information security as part of the overall organizational culture because they do not follow a holistic and integrated management approach [7].

Management's support of information security is an area that has been researched in many studies [9,10]. A major underlying problem with IT and systems risk is that managers are not knowledgeable of the full range of actions that they can take [10]. Because of this lack of knowledge by managers, subsequent plans of actions to cope with IT and systems risk have been less effective than they should be [14].

The Chief Information Officer (CIO) and Chief Information Security Officer (CISO) and their staffs also have a responsibility to better understand business functions and procedures to help align IT security to the organization's goals and business strategies. The CIO and CISO have the responsibility to make senior management aware of information security issues and to educate senior management on information security's relevance to the organization's strategic goals and business plans [17].

Another aspect of information security are new laws and regulations that have been enacted in recent years emphasizing information security and the role it plays within overall business processes [2,3]. Security concerns have become an integral part of our daily lives, and organizations need to ensure their information assets are adequately secured [13]. Federal, state, and local governments have enacted corporate governance regulations that encompass information security. More businesses are requiring assurances that their vendors and partners are properly protecting information assets from security risks and are taking measures to ensure business continuity.

IT governance efforts impact the success when trying to become compliant with local, state, and federal regulations based on the methodology, process, and approach an organization uses to become compliant. One study discussed three governance frameworks to help organizations achieve compliance: Control Objectives for Information and Related Technology (COBIT), Information Technology Infrastructure Library (ITIL), and ISO/IEC 17799:2000 [12]. Organizations must understand how to implement and incorporate these frameworks to their individual organization.

How do organizations determine the success of their information security culture? Should a successful information security culture be based on the organization not having a security breach or in terms of strategic value or various measures of business performance? An information security culture by itself will not keep an organization from having a security breach as technical controls also play a major role in keeping information secure. It is hard to measure the success of something that is designed to prevent an occurrence.. According to McFadzean, Ezingeard, and Birchall, the value of information security cannot be determined by strategic value or business performance measures [10]. This publication points out that the value of information security is based on the perception of risk and the overall strategic importance of IT within the organization. The key is to look at the information security culture by asking the following questions concerning an organization's information security culture. Does a culture of information security permeate the organization? Is the security of information a part of everything the organization does? Is information security a daily routine of every employee? A successful information security culture may be defined as a portion of the overall corporate culture where information security becomes as common and routine any other business aspect of the organization. In other words, information security becomes "institutionalized" [16].

Based on a review of scholarly literature, the authors identified five factors as key to the success of an organizations information security culture. We developed these factors into research questions as follows:

1. What, if any, relationship exists between the perception of Management's support of information security and the organization's information security culture?
2. What, if any, relationship exists between the perceived alignment of information security to business strategies, plans, and goals and the organization's information security culture?
3. What, if any, relationship exists between the perception of the technical staffs' understanding of business functions and alignment and the organization's information security culture?
4. What, if any, relationship exists between the perceived use of information technology and information security frameworks and the organization's information security culture?

5. What if any, relationship exists between the perception of the organization’s information security awareness programs and training and the organization’s information security culture?

Research Methodology

This study used a quantitative research methodology with descriptive analysis to identify relationships between independent variables and the dependent variable [8]. A survey is well suited for this purpose. There are four types of questions that surveys are useful in answering: classifier or background questions, multiple choice or closed-end questions, intensity questions, and free response or open-ended questions. The purpose of these questions is to understand the thoughts, feelings, perceptions, and behavior of individuals [1]. A survey is a good method of collecting the perceptions of individuals on particular concepts. Quantitative research and factor analysis were used to determine the effect of these factors on developing and maintaining a successful information security culture.

This research study assisted in determining the degree that each of these factors affects an organizational information security culture’s success. The study surveyed random samples of United States organizational managers, IT professionals, and knowledge workers in order to gather the necessary data. The survey was Internet based using targeted survey panelists that met the criteria of manager, IT professional, or knowledge worker within the United States.

The survey gathered Likert scale responses to survey questions on information as well as demographic data. The research questions were tested using the Chi Square Test of Independence. The significance level for the Chi Square Test of Independence was set at 0.05. Additional analysis was conducted to determine if there was evidence that the type of industry, size of the organization, position of the individual within the organization, gender, or number of years an individual had been in the organization made a difference on the participant’s perception that a successful information security culture existed within the organization.

Bivariate correlation was used to determine the relationship between each of the independent variables and dependent variable. A positive relationship was indicated by a positive result in the bivariate correlation coefficient, while a negative relationship was indicated by a negative bivariate correlation coefficient. The closer the bivariate correlation coefficient was to +1 or –1, the stronger the relationship between the variables. A bivariate correlation coefficient that is closer to zero indicates a weak relationship between variables.

Quantitative Survey Results

The demographics of the usable surveys are broken out as follows.

Table 1. Gender

Gender	Number of Participants	Percentage of Participants
Male	142	71%
Female	58	29%

Table 2. Position within the Organization

Position	Number of Participants	Percentage of Participants
Manager	83	41.5%
IT Professional	27	13.5%
Knowledge Worker	90	45%

This break out of positions is in line with the expectations of the research study, although the percentage of manager positions was somewhat higher than expected.

Table 3. Size of the Organization

Size of the Organization	Number of Participants	Percentage of Participants
1 to 25	25	12.5%
26 to 100	16	8%
101 to 250	61	30.5%
Over 250	98	49%

The break out of the size of the organizations was within the research study's expected range.

Table 4. Years within the Organization

Years within the Organization	Number of Participants	Percentage of Participants
Less than 1	18	9%
1 to 3	35	17.5%
3 to 7	54	27%
Greater than 7	93	46.5%

This was within the research study's expectations.

Table 5. Type of Industry

Type of Industry	Number of Participants	Percentage of Participants
Financial	13	6.5%
Government	88	44%
Services	22	11%
Manufacturing	20	10%
Merchandise/Sales	5	2.5%
Education	21	10.5%
Other	31	15.5%

These numbers were within the study's expectations, with the government numbers being slightly higher than expected.

Using the Chi Square Test of Independence, the Case Processing Summary for the second research question is presented in Table 6, with the results of each survey question analyzed in Tables 7 through 10. The second research is: What, if any, relationship exists between the perceived alignment of information security to business strategies, plans, and goals and the organization's information security culture?

Table 6. Case Processing Summary for Research Question 2

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Q1 * Q5	200	100.0%	0	.0%	200	100.0%
Q2 * Q5	200	100.0%	0	.0%	200	100.0%
Q3 * Q5	200	100.0%	0	.0%	200	100.0%
Q4 * Q5	200	100.0%	0	.0%	200	100.0%

Table 7. Chi Square Test: First Survey Question, Research Question 2

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	1.390E2	16	.000
Likelihood Ratio	76.991	16	.000
Linear-by-Linear Association	38.152	1	.000
N of Valid Cases	200		

a. 16 cells (64.0%) have expected count less than 5. The minimum expected count is .05.

Table 8. Chi Square Test: Second Survey Question, Research Question 2

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	1.200E2	16	.000
Likelihood Ratio	77.453	16	.000
Linear-by-Linear Association	43.561	1	.000
N of Valid Cases	200		

a. 16 cells (64.0%) have expected count less than The minimum expected count is .08.

Table 9. Chi Square Test: Third Survey Question, Research Question 2

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	1.485E2	16	.000
Likelihood Ratio	77.004	16	.000
Linear-by-Linear Association	40.249	1	.000
N of Valid Cases	200		

a. 14 cells (56.0%) have expected count less than 5. The minimum expected count is .05.

Table 10. Chi Square Test: Fourth Survey Question, Research Question 2

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	1.419E2	16	.000
Likelihood Ratio	71.112	16	.000
Linear-by-Linear Association	52.627	1	.000
N of Valid Cases	200		

a. 16 cells (64.0%) have expected count less than 5. The minimum expected count is .05.

The Chi Square Test of Independence for each of the measurement questions related to the second research question had a significance value of .000. The results would indicate the two variables are associated; therefore, whether or not the organization has a successful information security culture would appear to depend on the alignment of information security to business strategies, plans, and goals.

This process was repeated for each of the research survey's questions as they related to their specific research question. In each case, the Chi Square Test of Independence for each survey question relating to its specific research question had a significance value of .000. Therefore, each independent variable is associated with the dependent variable, defined as a successful organizational information security culture.

The Bivariate correlation was used to determine the relationship between each of the independent variables and the dependent variable. Each question associated with a specific research question was tested with the dependent variable to determine a positive or negative correlation and the strength of the correlation.

Table 11. Bivariate Correlation: Survey Question 6, Research Question 3

		Q5	Q6
Q5	Pearson Correlation	1.000	.375**
	Sig. (2-tailed)		.000
	N	200	200
Q6	Pearson Correlation	.375**	1.000
	Sig. (2-tailed)	.000	
	N	200	200

**. Correlation is significant at the 0.01 level (2-tailed).

The results in Table 11 show there is a significant correlation between the sixth research question and the dependent variable as the significant coefficient yielded a value of .000. The correlation value was calculated at .375 which indicates a moderately positive relationship between this question and the dependent variable.

Table 12. Bivariate Correlation: Survey Question 7, Research Question 3

		Q5	Q7
Q5	Pearson Correlation	1.000	.533**
	Sig. (2-tailed)		.000
	N	200	200
Q7	Pearson Correlation	.533**	1.000
	Sig. (2-tailed)	.000	
	N	200	200

**. Correlation is significant at the 0.01 level (2-tailed).

Table 12 revealed a significant correlation between the seventh research question and the dependent variable. The correlation value was .533 which indicates a positive relationship between this question and the dependent variable. This relationship was stronger, but still only moderate.

Table 13. Bivariate Correlation: Survey Question 8, Research Question 3

		Q5	Q8
Q5	Pearson Correlation	1.000	.401**
	Sig. (2-tailed)		.000
	N	200	200
Q8	Pearson Correlation	.401**	1.000
	Sig. (2-tailed)	.000	
	N	200	200

**. Correlation is significant at the 0.01 level (2-tailed).

The results shown in Table 13 indicate a significant correlation existed between the eighth research question and the dependent variable. The correlation value was .401 which indicates a moderately positive relationship between this question and the dependent variable.

Table 14. Bivariate Correlation: Survey Question 9, Research Question 3

		Q5	Q9
Q5	Pearson Correlation	1.000	.435**
	Sig. (2-tailed)		.000
	N	200	200
Q9	Pearson Correlation	.435**	1.000
	Sig. (2-tailed)	.000	
	N	200	200

**. Correlation is significant at the 0.01 level (2 tailed).

There is a significant correlation indicated between the ninth research question and the dependent variable. The correlation value was .435, a moderately positive relationship between this question and the dependent variable.

Table 15. Bivariate Correlation: Survey Question 10, Research Question 3

		Q5	Q10
Q5	Pearson Correlation	1.000	.468**
	Sig. (2-tailed)		.000
	N	200	200
Q10	Pearson Correlation	.468**	1.000
	Sig. (2-tailed)	.000	
	N	200	200

**. Correlation is significant at the 0.01 level (2-tailed).

There was a significant correlation between the tenth research question and the dependent variable. The correlation value was .468, indicating that there was a moderately positive relationship between this question and the dependent variable.

All of the survey questions pertaining to Research Question 3 indicated that there was a significant relationship between Research Question 3 and the dependent variable. This relationship was positive, but moderate. Therefore, a positive relationship existed between the perception of the technical staffs' understanding of business functions and alignment and the success of the organization's information security culture, although moderate evidenced by the average correlation value of .442.

The same procedure was conducted on each survey question as related to each of the research questions. The survey questions that related to Research Question 1, management support of information security, all had a significant relationship to the dependent variable. The correlation values were positive ranging from .464 to .604, with one exception. Survey question 27 showed a negative correlation. This question was worded in a manner in which one would disagree or strongly disagree if the perception was that management cares about information security, as stated in the question, "My company's managers only care about information security when there is a breach of security." Therefore, a negative correlation would be expected only if the perception was that management cares about information security all the time. The correlation value for question 27 was -.339. The average correlation value for Research Question 1 was .500 if the correlation value of question 27 is considered positive. These correlation values showed a moderate relationship between Research Question 1 and a successful organizational information security culture.

The survey questions that related to Research Question 2, alignment of information security to business, all had a significant relationship to the dependent variable. The correlation values were positive, ranging from .438 to .514. The average correlation value for Research Question 2 was .468. This indicated a moderate relationship between the research question and a successful organizational information security culture.

The related survey questions to Research Question 4, stated as the "use of IT and information security frameworks", had a significant relationship to the dependent variable. The correlation values for these survey questions were positive, ranging from .565 to .616. The average correlation value for Research Question 4 was .585.

The survey questions that related to Research Question 5, training and awareness programs, showed a significant relationship to the dependent variable. The correlation values for these survey questions were positive and ranged from .567 to .645. Although still moderate, they were the highest for all of the research questions, with an average correlation value of .600.

The demographic questions were also analyzed to see if there was any relationship between a specific demographic and the success of an organization's information security culture. Only one of the demographic questions showed a significant relationship to the dependent variable, that being demographic question 3, defining the size of the organization. This question had a significant coefficient of .004, which is less than .01. The correlation value for the size of the organization was .203, exhibiting a weak relationship. Therefore, the size of the organization had a positive but weak relationship to the perceived success of an organization's information security culture.

Analysis of Results

Based on the analysis of the data, the research found that a positive relationship exists between the research questions and the success of an organization's information security culture. However, the strength of the relationships was not as strong as these researchers had expected, with strength ranging from a low-moderate to high-moderate relationship.

The research questions were ranked from the strongest relationship to the weakest as follows:

Table 16. Rank of Research Questions from Strongest to Weakest Relationship

Research Question Number	Research Question Topic	Average Correlation Value
RQ5	Information Security Training and Awareness Programs	.600
RQ4	Use of IT and Information Security Frameworks	.585
RQ1	Management Support of Information Security	.500
RQ2	Alignment of Information Security to Business	.468
RQ3	Technical Staff's Understanding of Business Functions and Alignment	.442

According to this data and analysis outcome, information security training and awareness programs had the strongest positive relationship to an organization's successful information security culture. The technical staff's understanding of business functions and alignment had the weakest positive relationship to a successful information security culture.

Conclusions

This research study reviewed the existing body of knowledge to determine what factors were indicated in playing a key role in the success of an organizational information security culture. In order to determine if the factors had a positive relationship to a successful information security culture, the research study developed a survey instrument to measure the perception of the independent variables and their relationship to the dependent variable. The survey instrument was validated through a field test to determine reliability and validity. Following the validation of the study instrument, the survey was subjected to a pilot study to confirm reliability and then opened to the sample population for the full study.

The data collection phase gathered 200 usable surveys that were completed by organizational managers, IT professionals, and knowledge workers. Their responses were collated and an analysis of the results indicated that there was a significant positive relationship between the five factors and a successful organizational information security culture.

This study indicated that these five factors had a significant and positive relationship to a successful organizational information security culture. The research effort provided information that researchers can build upon. Additionally, this study provided practitioners with information on how to prioritize and focus their efforts and resources in implementing, integrating, and maintaining a successful information security culture in order to protect the organization's information assets.

References

[1] Aiman-Smith, L., & Markham, S. (2004). What you should know about using surveys. *Research Technology Management, 47*(3), 12-15. Retrieved from Business Source Complete database.

[2] Barry, G., & Grossmeier, J. (2009, July). Is your incentive strategy sound? Guidelines for designing a HIPAA compliant wellness program. *Employee Benefit Plan Review, 64*(1), 5-8. Retrieved from ABI/INFORM Global database.

[3] Damianides, M. (2005). Sarbanes-Oxley and IT governance: New guidance on it control and compliance. *Information Systems Management, 22*(1), 77-85. Retrieved from ABI/INFORM Global database.

[4] Deal, T. E., & Kennedy, A. A. (1982). *Corporate cultures*. Reading, MA: Addison-Wesley.

[5] Deshpande, R., & Farley, J. U. (1999). Executive insights: Corporate culture and market orientations: Comparing Indian and Japanese firms. *Journal of International Marketing, 7*(4), 111-127. Retrieved from ABI/INFORM Global database.

[6] Freeman, E. H. (2007, September). Holistic information security: ISO 27001 and due care. *Information Systems*, *16*(5), 291-294. Retrieved from ABI/INFORM Global database.

[7] Grobler, T, & Louwrens, B. (2005). New information security architecture. *Information Security of South Africa (ISSA).* Retrieved from http://icsa.cs.up.ac.za/issa/2005/proceedings /full/046_article.pdf.

[8] Hopkins, W. G. (2008). Research designs: Choosing and fine-tuning a design for your study. *Sportscience 12*, 12-21. Retrieved from http://www.sportsci.org/2008/ wghdesign.pdf.

[9] Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: Management's effect on culture and policy. *Information Management & Computer Security, 14*(1), 24-36. Retrieved from ABI/INFORM Global database.

[10] McFadzean, E., Ezingeard, J. N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review, 31*(5), 622. Retrieved from ABI/INFORM Global database.

[11] Rashid, M. Z. A., Sambasivan, M., & Johari, J. (2003). The influence of corporate culture and organisational commitment on performance. *The Journal of Management Development 22*(7/8), 708-728. Retrieved from ABI/INFORM Global database.

[12] Robinson, N. (2005). IT excellence starts with governance. *The Journal of Investment Compliance*, *6*(3), 45-49.

[13] Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal, 39*(4), 60-62, 64-66. Retrieved from ABI/INFORM Global database.

[14] Straub, W. & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469. Retrieved from ABI/INFORM Global database.

[15] Van Niekerk, J. & Von Solms, R. (2005). An holistic framework for the fostering of an information security sub-culture in organizations. *Information Security of South Africa (ISSA).* Retrieved from http://icsa.cs.up.ac.za/issa/2005/proceedings/full/041_article.pdf.

[16] Von Solms, R. (1998). Information security management (1): Why information security is so important. *Information Management & Computer Security, 6*(4), 174-177. Retrieved from ABI/INFORM Global database.

[17] Whitten, D. (2008). The chief information security officer: An analysis of the skills required for success. *The Journal of Computer Information Systems, 48*(3), 15-19. Retrieved from ABI/INFORM Global database.

[18] Zakaria, O. (2004). Understanding challenges of information security culture: A methodological issue. *Proceedings of the Second Australian Information Security Management Conference, Perth, Australia*. Retrieved from http://scholar.google.com/scholar?hl=en&q=%22Omar+Zakaria %22&btnG=Search&as_sdt=0%2C11&as_ylo=&as_vis=0. (10.1.1.60.5059.pdf)