International Journal of Psychology and Cognitive Science
2019; 5(1): 9-23
http://www.aascit.org/journal/ijpcs
ISSN: 2472-9450 (Print); ISSN: 2472-9469 (Online)

American Association for Science and Technology

Organizational Factors Affecting Information Security Management Practices in Private Sector Organizations

Abdulrahman Ali Mohsen Al-Harethi[1, *], Abdullah Hussein Abdullah Al-Amoodi[2]

[1]Department of Project Management, Limkokwing University of Creative Technology, Cyberjaya, Malaysia
[2]Department of Computing, Universiti Pendidikan Sultan Idris (UPSI), Tanjong Malim, Malaysia

Email address

alharethi1992@gmail.com (A. A. M. Al-Harethi), Abdullah_alamoodi@outlook.com (A. H. A. Al-Amoodi)
[*]Corresponding author

Citation

Abdulrahman Ali Mohsen Al-Harethi, Abdullah Hussein Abdullah Al-Amoodi. Organizational Factors Affecting Information Security Management Practices in Private Sector Organizations. *International Journal of Psychology and Cognitive Science.* Vol. 5, No. 1, 2019, pp. 9-23.

Received: December 25, 2018; **Accepted**: January 23, 2019; **Published**: January 31, 2019

Abstract: The objective of this study is to address a comprehensive framework for managers and IT employees towards better information security management which boosts their awareness to a better level. A quantitative survey is conducted in order to investigate the information security element in technical IT departments of the private sector organizations in the kingdom of Saudi Arabia and to boost the security awareness among managers and IT staff of those chosen organizations. The results suggest that the more experienced and aware the staff get, the less of damages that will occur in the company, also it will enhance the organization overall information security policies. The research limitations are lack of ISM analysis Studies conducted in Saudi Arabia considering the private sector. Some respondents refused to cooperate in filling the survey, while some thought that their participation will reflect on their job and it might show to others their inexperience skills. The study only covered private sector organizations in Jeddah, Saudi Arabia. A proposed framework will be detailed and evaluated. Recommendations will be addressed to the staff and managers to help them evolve their awareness of IS and managing it. Findings are aimed to benefit IS managers; enable them to realize ways to boost security awareness. The study will add some contribution to ISM researches and the main body of knowledge.

Keywords: Information Security Awareness (ISA), Information Security Management (ISM), Private Sector Organizations, Saudi Arabia, Security Components

1. Introduction

The world is witnessing dramatic advancement in the information transmission ratio as well as the vast increase in the communication media. All those create the need for a higher level of information security for all types of use. it also indicates that security is becoming a serious area of interest to organizations rather than being only a step they need implementing to keep with the latest technological trends [1]. There are a variety of causes which cause this need such as: dealing with sensitive business information owned by companies and managing it in the marketplace, also having single document policy which interacts with different types of users and tries to deal with their issues all in the same sense [2].

There are various definitions for the notion “Information security”. Alijifri and Navaro [3] defined it as the major protection of information from being compromised in any way, along with ensuring it remains available, confidential and integer in the same time. When it concerns the management and security together, Lewis shared he believes that it’s more to having proactive management for the security vulnerabilities and it should be based on daily business operations [3]. It’s usually involving legislation and access control through policies which determine who should be allowed to access it and to which extent. Not to mention the management role in the discipline in which plays an ultimate factor towards controlling its risks to the nature of the business [4]. With the vast increase of information security's need in the market, the companies compete to maintain enough financials to keep up with latest technologies trends, which will profit the business as well as maintaining the resources considering the continuous adjustments to the market nature.

The role of information technology shall assist the staff along with the management to deal with obstacles that the organization will inevitably face, even if the challenges are brand new, it's still solvable in the right time and the organizational survival shall continue. Saudi Arabia is contributing a lot of financial resources to become one of the best IT vendors in the near future. The country is rapidly evolving its IT adoption to support the economy, as well as its technology related to future plans. The use of IT is increasing in Saudi to a great level. According to Go-Gulf Blog [5], the individuals in Saudi Arabia are ranked seventh around the world for social media accounts along with 20.9 active million users on the internet [6].

As part of the country's transformation and according to the ministry of Communication and Information Technology for their 2030's vision, the ministry has set some objectives for their IT adoption and enhancement in the IT field. They expect to develop and enable smart government operations based on common infrastructures. Both government and private sectors will increasingly rely on IT usage which enables them to keep up with technology as well as benefitting them and improve their economy [7].

Recently, many organizations are competing in the race of implementing IT without proper planning or understanding to security-related risks. The normal staffs have limited knowledge for the security requirements. In many incidents, when staffs are trying to understand and act accordingly, they end up with the most complicated solutions. However, the future also suggests that the challenges to information security which are faced by security managers will play an important role if not the most important one in determining the company's survival and success. It's not sufficient that organizations only manages information security by focusing on the technicality and forget all other aspects, the company cannot turn a blind eye on the social issue since the system we are dealing with is operated and used by people [8]. Organizations around the globe are starting to notice the ambiguous damages and effects of the security breaches due to the rise in productivity and accessibilities. For that, many organizations have started embracing awareness security programs. It takes lots of uniformity as well as promptitude by both administrations and employees of an organization to integrate the information security to the organizational strategic planning. Especially in the midst of the business process which will result in determining the organizational success or failure [9].

Information security is considered the barrier that shields out data privacy; it deals with security vulnerabilities as they happen. Some of these vulnerabilities are results of the insufficient way the organizations handle the data. The lack of proper planning is another cause in this scenario. Thereby, it became a serious concern that organizations are ought to continuously apply risk analysis which will play an astonishing role in maintaining data and guarding their system.

Saudi Aramco, one of the greatest oil production companies in the world was attacked by a virus named "Shamoon". The Middle East has more than half of the oil productions globally along with natural gas, which makes this region an area of interest to security cyber-attacks. According to the United States Department of defense, while addressing the security of the Gulf countries "Some of them are in good shape, Saudi Arabia is not". All of the damages caused could have been avoided only if there was proper compliance with some basic security requirements, awareness, and managerial supervision.

Organizational success is influenced by the level of financial resources the organizations are willing to invest in their information security [10]. Some of them with insufficient financials in the IS are less functional compared with others. That is due to the rapid change in ICT, and that have revealed some security Vulnerabilities associated with organizational data protection [8]. Organizations are obligated to implement effective security programs to maintain their valuable data since the technical and management roles are not only enough to face cyber threats. Therefore the organizations must determine what information must be protected and to which extent, and to enable better security programs and legislation [11]. In general, organizations are focusing their resources on external risks and turn a blind eye on the fact that there could be serious vulnerabilities within the organization and its practices [12]. The organizations can be harmed severely due to some factors such as; employees unawareness, insufficient information security legislation, and policies. Thus, it's a duty and role of the Information technology departments within these organizations to investigate the causes which affect the security management for their information [12]. Based on that, this research tries to answer the following question:

1. What are the factors that influence information security management in the private Information Technology sector Organizations in the kingdom of Saudi Arabia?
2. What is the information security development process for the managerial elements that influence information security management Among IT Managers and Staff and how they are linked?
3. How to increase IS awareness in Private Sector Organizations in the Kingdom of Saudi Arabia?

This study is targeting IT departments in the private sector organizations operating in Jeddah city in the Kingdom of Saudi Arabia. The study will rely on the quantitative approach to collect data from 150 participants working in different areas; the survey is conducted by distributing the samples through personal Interviews with participants. The sample used is based on previous studies and some questions will be added to widen the resulting scope of the expected findings. In addition, the Pearson correlation is conducted to test the correlation among information security elements.

The expected outcomes and findings of this study are aimed to benefit the managers of information security; it will enable them to realize ways to boost security awareness in the company. In addition, the results of this study will add some contribution to Information security management researches the main body of knowledge. Based on that, the main aim of this study is to identify key essential elements of information security management and its awareness. In addition, this study also examines essential information security management factors which have influence over the Private IT sector organizations in the Kingdom of Saudi Arabia. Moreover, to propose an information security framework and evaluate it based on managerial factors to boost security awareness among IT managers and staff. Lastly, to suggest some recommendations that will enhance security awareness among organization managers and employees within information security areas.

2. Literature Review

Administrations in various industries have known for a long time that information security is a serious contributor to their business's success. However; they dealt with this on the basis that it's only a technologically driven and ignored the fact that it could also be business driven. This concept has changed in recent years as many organizations and due to security breaches have established their administrative control based on those incidents they came across [13]. The organization's management is the main point to ensure the best information security practice; it helps the organization to accomplish its objectives. The management in the area of information security is also considered the functional party who controls the organizational assets. Therefore, it has a duty to put it at disposal to the best ways that serve the best interest of the organization. Moreover, the management also has a duty to ensure the best risk management planning for all the company's divisions [14].

2.1. Information Security Management

The Information Security Management Concept (ISM) is defined as the systematic managerial role over the business risks, it investigates, observe, manage and maintain the best state of the information security as well as improving it. In any business nature, the existence of security management has its unique way of identifying its related needs based on the business. Sometimes it's determined by the complexity and scope that the business is meant for. ISM involves multiples components such as security policy, individual security both physical and environmental, corporation security, access control, resources control and classification, operational management, and communication, system development and maintenance along with business continuity management [15].

2.2. Related Works (ISM)

Table 1. *ISM Related Works.*

Reference	Article title	Highlights
[16]	An information security knowledge sharing model in organizations	A model to minimize the occurrences of information security breaches
[17]	Developing a Theory-based Information Security Management Framework for Human Service Organizations	the framework of information security management to target the Human service organizations
[18]	Information security and business continuity management in inter-organizational IT relationships	Investigates the approaches embraced by IT managers To provides better business management
[19]	Identifying factors of "organizational information security management"	Identifying information security management elements that influence organizations and their security
[20]	Modeling of information security management parameters in Indian organizations using ISM and MICMAC approach	Framework for different factors that influence information security management
[21]	Identifying core control items of information security management and improvement strategies by applying fuzzy DEMATEL	Information security domains and effects factors that influence their relations
[22]	An information security risk-driven investment model for analyzing human factors	The risk-driven model that investigate human factors and security concerns they caused in organizations
[23]	The Human Factor of Information Security: Unintentional Damage Perspective	Examining the factors affecting IS and lead to unpredictable danger to organizations and their assets
[24]	Comparing the information security culture of employees who had read the information security policy and those who had not	compare IS a culture of staff with security knowledge compared with other staff with no prior knowledge

2.3. Awareness

IS awareness is a large contributor within the industry and many international standards have shade lights on its importance such as ISO27001, COBIT, Payment Card Industry and ISO 9001.2000 [25]. The importance of information security awareness depends on its measures to elevate IS system and to prevent security breaches [26]. The awareness of IS affects the behavioral changes among employees while boosting the security activities; it also enables them to be more responsive to the security solutions which start a cultural change in the organization

[1].

IS integration with awareness must be a continuous process to avoid serious problems which are usually caused by the incompetence level of staff awareness's knowledge. For example, between May 2004 and May 2005 around 1.2 million computer users experienced losses due to phishing attacks in the United States which valued at $929 million. The awareness training is not meant to entertain employees and keep them from doing their tasks and duties within working hours, it's simply about security to be delivered to more audience to and to enable them to avoid the possible security breaches [27].

For successful awareness within any business environment, some awareness approaches have been introduced. The aim of these approaches is to ensure all the employee's awareness compliance is in the best shape in order for them to skip the information security risks associated with the human factor. According to Cone et al. [28], the approaches differ in their delivery means along with the tools used to instruct those, including official practice sessions, online-based training, and computer-based training. Ahlan, Lubis, and Lubis [29] have carried out a study to create a new model which deeply evaluates the significance of three factors on ISA: Individual, Institutional and Environmental. Their study is a continuation of research based on responsibility and consequences for ISA over technical errors and data modification in the collection stage [30].

2.4. Related Work Awareness

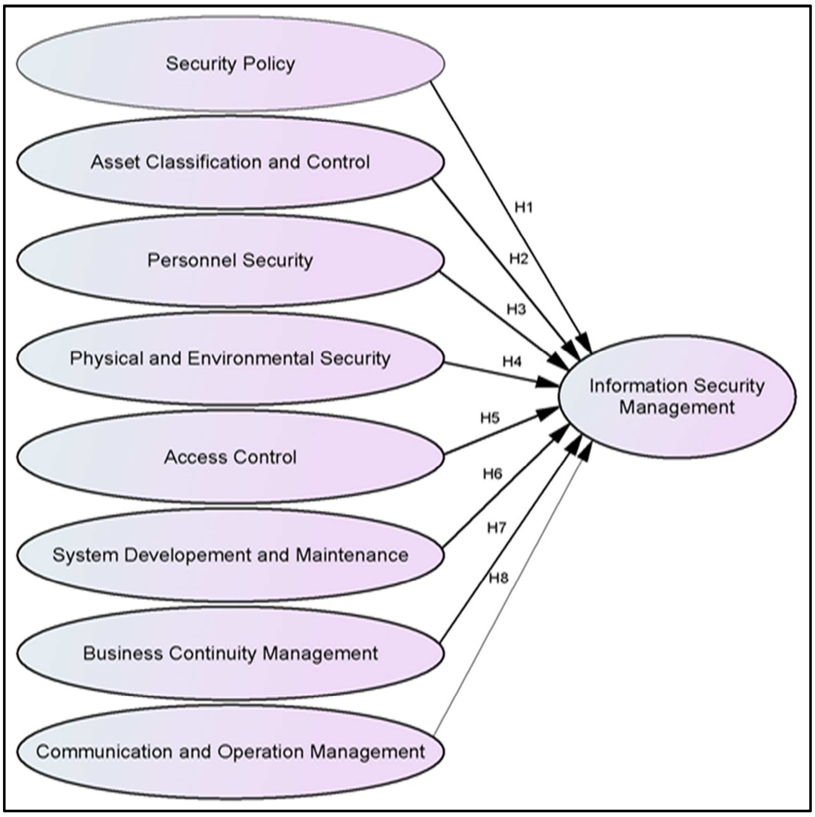
Security Policy
Asset Classification and Control
Personnel Security
Physical and Environmental Security
Access Control
System Developement and Maintenance
Business Continuity Management
Communication and Operation Management
H1
H2
H3
H4
H5
H6
H7
H8
Information Security Management

Figure 1. *Research Proposed Model.*

Table 2. *ISA Related Work.*

Reference	Article title	Highlights
[31]	Analyzing trajectories of information security awareness	Importance of management and organizational perspective in information security awareness
[32]	Persona-Driven Information Security Awareness	Information security awareness model based on the personas scheme
[33]	A Study of Information Security Awareness and Practices in Saudi Arabia	Information security awareness practices in the kingdom of Saudi Arabia
[34]	Exploring the relationship between student mobile information security awareness and behavioral intent	Examining the relationships between students cell-phone ISA with behavioral objectives

Based on the above, this study proposes the following hypotheses and framework:

1. H1. Security Policy has a positive significant relationship with Information Security Management practices within private sector organizations in Saudi Arabia.
2. H2. Asset Classification and Control has a positive significant relationship with Information Security

Management practices within private sector organizations in Saudi Arabia.

3. H3. Personnel Security has a positive significant relationship with Information Security Management practices within private sector organizations in Saudi Arabia.
4. H4. Physical and Environmental Security has a positive significant relationship with Information Security Management practices within private sector organizations in Saudi Arabia.
5. H5. Access Control has a positive significant relationship with Information Security Management practices within private sector organizations in Saudi Arabia.
6. H6. System Development and Maintenance have a positive significant relationship with Information Security Management practices within private sector organizations in Saudi Arabia.
7. H7. Business Continuity Management has a positive significant relationship with Information Security Management practices within private sector organizations in Saudi Arabia.
8. H8. Communication and Operation Management has a positive significant relationship with Information Security Management practices within private sector organizations in Saudi Arabia.

3. Methodology

For the purpose of this study, quantitative research methodology is selected to conduct the exploratory study. This type of methodologies is based on counting and evaluating things, then come up with different estimations on different groups. On the other hand, the qualitative research methodology has an essential role in social science and more focused on the cause behind people behavior, knowledge, faiths and responsibilities. This research employs the quantitative research methodology. In order to meet with this research objectives, next figure displays the operational framework for this study.

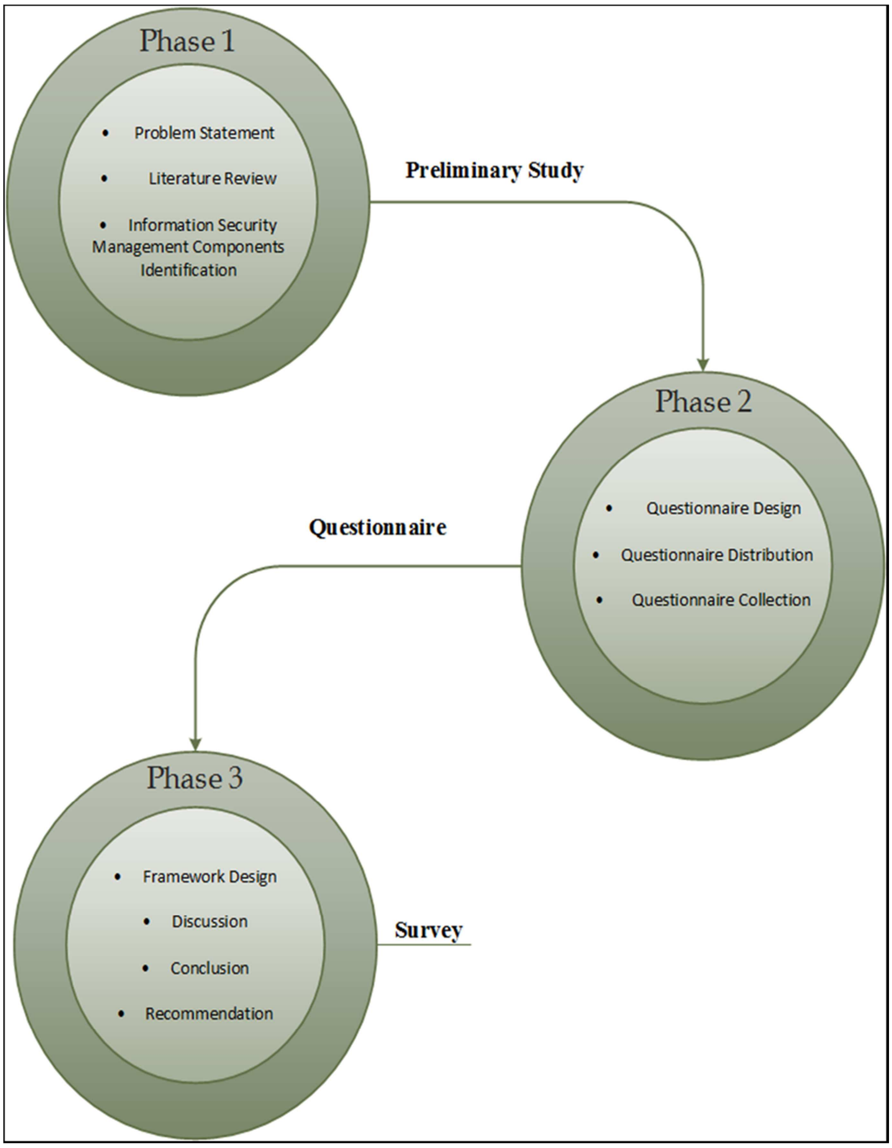

Figure 2. Research Framework.

The participants of this study are employees along with Information security managers of IT departments of Private sector organizations in Jeddah City, Saudi Arabia. The researcher's objective is to gather 150 valid samples from different participants in that region. In order to meet with this study's objectives, the questionnaire was designed in a way which allows us to point out the factors that have its own influence over the information security management in the IT departments for private sector organizations in the Kingdom of Saudi Arabia. In order to discover the affecting factors we mentioned previously, this study is proposed the following variables extracted from previous literature including: security policy, asset classification and control, personnel security, physical and environmental security, communications and operations management, access control, system development and maintenance, business continuity management.

Table 3. *Components of the Study.*

Section	Title
I	Personnel / Individual security
II	Security Policies
III	Physical and Environmental security
IV	Assets classification and control
V	Communication and Operations Management
VI	Business Continuity Management
VII	Access Control
VIII	System Development and Maintenance

After gathering all the data from the participants, a statistical analysis will be performed using the SPSS Statistics application. The analysis will be conducted by using frequency, descriptive analysis, and reliability assessments by utilizing Cronbach's alpha and correlation analysis to make the data analysis. Various kinds of rating scales have been developed to measure attitudes directly. The most widely used is the Likert Scale. Likert scale (1932) was developed based on the principle of measuring attitudes by asking people to respond to a series of statements about a certain topic, in terms of the extent to which they agree with them, and so tapping into the cognitive and affective components of attitudes.

Table 4. *Likert Scale table.*

Agreement	Frequency
Strongly Agree	Very Frequently
Agree	Frequently
Undecided	Occasionally
Disagree	Rarely
Strongly Disagree	Never

4. Findings & Discussions

In this study, 150 questionnaires were distributed among IS managers and IT staff in private sector organizations operating in Jeddah, Kingdom of Saudi Arabia. All the questionnaires were given and collected within the same business day in arrangement with the Organizations administrations. All the 150 surveys results have been entered and used to conduct the data analysis. The instrument of the survey is a self-administrated questionnaire which has been circulated to fit the sample of the study.

4.1. Reliability Analysis

It is concluded that all the components in this study are considering the fact that all their alpha values are equal or greater than 0.65. In other words, the internal consistency reliability of the measures used in this study is considered to be acceptable and good as shown in the following table.

Table 5. *Reliability Analysis.*

Variables	Number of Components	Alpha
security policy	5	0.73
Organizational security	3	0.75
Asset Classification and Control	3	0.69
Personnel security	3	0.79
Physical and environmental security	5	0.72
Communications and operations management	6	0.66
Access control	4	0.69
System development and maintenance	2	0.71
Business continuity management	3	0.65

4.2. Descriptive Analysis

In order to gain a better understanding of descriptive analysis's results, every main variable is categorized into three levels; low (for all answers which disagrees or strongly disagrees), moderate and high (for all answers which either agrees or strongly agrees.

Mean value is used to describe the average number of respondents who agreed on the influencing factors engagement that had been identified in the literature review. The mean raking of each item was analyzed in order to determine its central tendency. The central tendency level will identify whether the items are in the range of low, medium or high.

Table 6. *Mean Score Calculation.*

Mean Range	Level of Acceptance
High	3.8 – 5.00
Medium	2.4 – 3.7
Low	1.00 – 2.3

After analyzing the data of the questionnaire questions, the researcher dealt with the results of the responses of the sample for the terms of the survey questions. After unloading the questionnaire data in the SPSS program, the results were shown as the following:

Table 7. *Factors' Descriptive Analysis.*

Variable	Mean	St Deviation	Level of Acceptance	Mean Score Representation
Security Policy	3.7466	0.878099	High	3
Asset Classification & Control	3.398	0.970925	Moderate	8
Personnel Security	3.764	0.866663	High	2
Physical & Environment Security	3.5702	0.949454	Moderate	6
Access Control	3.85325	0.844128	High	1
System Development & Maintenance	3.527	0.895082	Moderate	7
Business Continuity Management	3.728	0.867534	High	5
Communication & Operation Management	3.7325	0.843842	High	4

4.3. Correlation

The Correlation matrix below displays correlation between our survey independent variables (security policy, asset classification and control, personnel security, physical and environmental security, communication and operation management, access control, systems development, and maintenance and business continuity management) and the dependent variable (Information Security Management. In other words, this correlation is conducted using Pearson approach in order to inspect how the variables would independently correlate with each other and with the dependent variable and to what extent.

4.3.1. Security Policy and ISM Correlation

Table 8. *SP & ISM Correlation.*

		SP	ISM
SP	Pearson Correlation	1	.387**
	Sig. (2-tailed)		.000
	N	150	150
ISM	Pearson Correlation	.387**	1
	Sig. (2-tailed)	.000	
	N	150	150

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

There was a positive correlation between security policies and information security management, r = 0.387, n = 150, p = 0.000. In general, there was a low, positive correlation between security policy and information security management. The Increases in security policy were correlated with increases in information security management.

4.3.2. Asset Classification and Control and ISM Correlation

Table 9. *ACC & ISM Correlation.*

		ACC	ISM
ACC	Pearson Correlation	1	.619**
	Sig. (2-tailed)		.000
	N	150	150
ISM	Pearson Correlation	.619**	1
	Sig. (2-tailed)	.000	
	N	150	150

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

There was a positive correlation between Asset Classification and Control and information security management, r = 0.619, n = 150, p = 0.000. In general, there was a moderate, positive correlation between Asset Classification and Control and information security management. The Increases in Asset Classification and Control were correlated with increases in information security management.

4.3.3. Personnel Security and ISM Correlation

Table 10. *PS & ISM Correlation.*

		PS	ISM
PS	Pearson Correlation	1	.341**
	Sig. (2-tailed)		.000
	N	150	150
ISM	Pearson Correlation	.341**	1
	Sig. (2-tailed)	.000	
	N	150	150

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

There was a positive correlation between Personnel Security and information security management, r = 0.341, n = 150, p = 0.000. In general, there was a low, positive correlation between Personnel Security and information security management. The Increases in Personnel Security were correlated with increases in information security management.

4.3.4. Physical and Environmental Security and ISM Correlation

Table 11. *PES & ISM Correlation.*

		PES	ISM
PES	Pearson Correlation	1	.108
	Sig. (2-tailed)		.190
	N	150	150
ISM	Pearson Correlation	.108	1
	Sig. (2-tailed)	.190	
	N	150	150

There was no significance correlation between Physical and environmental security and information security management, r = 0.108, n = 150, p = 0.190. In general, there was a low, non-significance correlation between Physical and environmental security and information security management. The Increases in Physical and environmental security were not found to be significantly correlated with increases in information security management.

4.3.5. Access Control and ISM Correlation

Table 12. *AC & ISM Correlation.*

		AC	ISM
AC	Pearson Correlation	1	.396**
	Sig. (2-tailed)		.000
	N	150	150
ISM	Pearson Correlation	.396**	1
	Sig. (2-tailed)	.000	
	N	150	150

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

There was a positive correlation between Access Control and information security management, r = 0.396, n = 150, p = 0.000. In general, there was a low, positive correlation between Access Control and information security management. The Increases in Access Control were correlated with increases in information security management.

4.3.6. System Development and Maintenance and ISM Correlation

Table 13. *SDM & ISM Correlation.*

		SDM	ISM
SDM	Pearson Correlation	1	.036
	Sig. (2-tailed)		.658
	N	150	150
ISM	Pearson Correlation	.036	1
	Sig. (2-tailed)	.658	
	N	150	150

There was no significant correlation between System Development and Maintenance and information security management, r =.036, n = 150, p =.658. In general, there was a low, non-significance correlation between System Development and Maintenance and information security management. The Increases in System Development and Maintenance were not found to be significantly correlated with increases in information security management.

4.3.7. Business Continuity Management and ISM Correlation

Table 14. *BCM & ISM Correlation.*

		BCM	ISM
BCM	Pearson Correlation	1	.075
	Sig. (2-tailed)		.363
	N	150	150
ISM	Pearson Correlation	.075	1
	Sig. (2-tailed)	.363	
	N	150	150

There was no significant correlation between Business Continuity Management and information security management, r =.075 n = 150, p =.363. In general, there was a low, non-significance correlation between Business Continuity Management and information security management. The Increases in Business Continuity Management were not found to be significantly correlated with increases in information security management.

4.3.8. Communication and Operation Management and ISM Correlation

Table 15. *COM & ISM Correlation.*

		COM	ISM
COM	Pearson Correlation	1	.315**
	Sig. (2-tailed)		.000
	N	150	150
ISM	Pearson Correlation	.315**	1
	Sig. (2-tailed)	.000	
	N	150	150

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

There was a positive correlation between communication and Operation management and information security management, r = 0.315, n = 150, p = 0.000. In general, there was a low, positive correlation between communication and Operation management and information security management. The Increases in communication and Operation management were correlated with increases in information security management.

4.4. Regression/Hypotheses Testing Analysis

We are conducting this analysis using SPSS statistical application to test our previous 8 hypotheses and see if they are approved or not. Each independent variable (Hypotheses) will be analyzed with the only dependent variable (Information Security Management) to see the significance and how positively or negatively great it might be.

H1: Security Policy has a positive significant relationship with Information Security Management practices within private sector organizations in Saudi Arabia.

Table 16. *Security Policy's regression.*

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.020	.414		2.460	.015
	Security_Policy	.584	.114	.387	5.102	.000

a. Dependent Variable: Information_Security_Management

Table 17. *Security Policy ANOVA.*

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	21.562	1	21.562	26.028	.000^b
	Residual	122.605	148	.828		
	Total	144.167	149			

a. Dependent Variable: Information_Security_Management

b. Predictors: (Constant), Security_Policy

Simple linear regression was calculated to determine Information Security Management effects based on Security policy. A significance regression equation was identified (F (1,148) = 26.028, P <.000), with R^2 of .150. Participants organizations predicted that Information Security Management is equal to 1.020 +.584 (Security Policy). Participants' organization Information Security Management increases .584 for each 1 present increase of Security Policy. Therefore, H1 is accepted.

H2: Asset Classification and Control have a positive significant relationship with Information Security Management practices within private sector organizations in Saudi Arabia.

Table 18. *Asset Classification and Control Regression.*

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.952	.233		4.085	.000
	Asset_Classification_and_control	.674	.070	.619	9.581	.000

a. Dependent Variable: Information_Security_Management

Table 19. *Asset Classification and Control ANOVA.*

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	55.189	1	55.189	91.798	.000^b
	Residual	88.978	148	.601		
	Total	144.167	149			

a. Dependent Variable: Information_Security_Management

b. Predictors: (Constant), Asset_Classification_and_control

Simple linear regression was calculated to determine Information Security Management effects based on Asset Classification and Control. A significance regression equation was identified (F (1,148) = 91.798, P <.000), with R^2 of .383. Participants' organizations predicted that Information Security Management is equal to 0.952 +.674 (Asset Classification and Control). Participants' organization Information Security Management increases .674 for each 1 present increase of Asset Classification and Control. Therefore, H2 is accepted.

H3: Personnel Security has a positive significant relationship with Information Security Management practices within private sector organizations in Saudi Arabia

Table 20. *Personnel Security Regression.*

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.678	.331		5.063	.000
	Personnel_Security	.387	.088	.341	4.409	.000

a. Dependent Variable: Information_Security_Management

Table 21. *Personnel Security ANOVA.*

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	16.739	1	16.739	19.442	.000^b
	Residual	127.427	148	.861		
	Total	144.167	149			

a. Dependent Variable: Information_Security_Management

b. Predictors: (Constant), Personnel_Security

Simple linear regression was calculated to determine Information Security Management effects based on Personnel Security. A significance regression equation was identified (F (1,148) = 19.442, P <.000), with R^2 of .116. Participants' organizations predicted that Information Security Management is equal to 1.678 +.387 (Personnel Security). Participants' organization Information Security Management increases .387 for each 1 present increase of Personnel

Security. Therefore, H3 is accepted.

H4: Physical and Environmental Security has a positive significant relationship with Information Security Management practices within private sector organizations in Saudi Arabia.

Table 22. *Physical and Environmental Security Regression.*

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.640	.359		7.362	.000
	Physical_and_Environmental_Security	.135	.103	.108	1.316	.190

a. Dependent Variable: Information_Security_Management

Table 23. *Physical and Environmental Security ANOVA.*

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1.668	1	1.668	1.732	.190^{b}
	Residual	142.499	148	.963		
	Total	144.167	149			

a. Dependent Variable: Information_Security_Management
b. Predictors: (Constant), Physical_and_Environmental_Security

Simple linear regression was calculated to determine Information Security Management effects based on Physical and Environmental Security. However, the results were not found to be significant (F (1,148) = 1.732, P >.000), with R^2 of .012. Participants' organizations predicted that Information Security Management is equal to 2.640 +.135 (Physical and Environmental Security). Participants' organizations Information Security Management increase .135 for each 1 present increase of Physical and Environmental Security and therefore there is no significance. Therefore, H4 is rejected.

H5: Access Control has a positive significant relationship with Information Security Management practices within private sector organizations in Saudi Arabia.

Table 24. *Access Control Regression.*

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.952	.416		2.290	.023
	Access_Control	.574	.109	.396	5.249	.000

a. Dependent Variable: Information_Security_Management

Table 25. *Access Control ANOVA.*

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	22.626	1	22.626	27.551	.000^{b}
	Residual	121.541	148	.821		
	Total	144.167	149			

a. Dependent Variable: Information_Security_Management
b. Predictors: (Constant), Access_Control

Simple linear regression was calculated to determine Information Security Management effects based on Access Control. A significance regression equation was identified (F (1,148) = 27.551, P <.000), with R^2 of .157. Participants' organizations predicted that Information Security Management is equal to .952 +.574 (Access Control). Participants' organization Information Security Management increases .574 for each 1 present increase of Access Control. Therefore, H5 is accepted.

H6: System Development and Maintenance have a positive significant relationship with Information Security Management practices within private sector organizations in Saudi Arabia.

Table 26. *System Development and Maintenance Regression.*

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.966	.313		9.462	.000
	System_Developement_and_Maintenance	.039	.088	.036	.444	.658

Dependent Variable: Information_Security_Management

Table 27. *System Development and Maintenance ANOVA.*

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.191	1	.191	.197	.658^b
	Residual	143.975	148	.973		
	Total	144.167	149			

a. Dependent Variable: Information_Security_Management
b. Predictors: (Constant), System_Developement_and_Maintenance

Simple linear regression was calculated to determine Information Security Management effects based on System Development and Maintenance. However, the results were not found to be significant (F (1,148) =.197, P >.000), with R^2 of .001. Participants' organizations predicted that Information Security Management is equal to 2.966 +.039 (System Development and Maintenance). Participants' organization Information Security Management increases .039 for each 1 present increase of System Development and Maintenance and therefore there is no significance. Therefore, H6 is rejected.

H7: Business Continuity Management has a positive significant relationship with Information Security Management practices within private sector organizations in Saudi Arabia.

Table 28. *Business Continuity Management Regression.*

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.751	.392		7.024	.000
	Business_Continuity_Management	.095	.105	.075	.912	.363

a. Dependent Variable: Information_Security_Management

Table 29. *Business Continuity Management ANOVA.*

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.805	1	.805	.831	.363^b
	Residual	143.361	148	.969		
	Total	144.167	149			

a. Dependent Variable: Information_Security_Management
b. Predictors: (Constant), Business_Continuity_Management

Simple linear regression was calculated to determine Information Security Management effects based on Business Continuity Management. However, the results were not found to be significant (F (1,148) =.831, P >.000), with R^2 of .006. Participants' organizations predicted that Information Security Management is equal to 2.751 +.095 (Business Continuity Management). Participants' organization Information Security Management increases .095 for each 1 present increase of Business Continuity Management and therefore there is no significance. Therefore, H7 is rejected.

H8: Communication and Operation Management has a positive significant relationship with Information Security Management practices within private sector organizations in Saudi Arabia.

Table 30. *Communication and Operation Management Regression.*

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.148	.490		2.344	.020
	Communication_and_Operation_Management	.538	.133	.315	4.033	.000

a. Dependent Variable: Information_Security_Management

Table 31. *Communication and Operation Management ANOVA.*

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	14.275	1	14.275	16.265	.000^b
	Residual	129.892	148	.878		
	Total	144.167	149			

a. Dependent Variable: Information_Security_Management
b. Predictors: (Constant), Communication_and_Operation_Management

Simple linear regression was calculated to determine Information Security Management effects based on Communication and Operation Management. A significance regression equation was identified (F (1,148) = 16.265, P <.000), with R^2 of .099. Participants' organizations predicted that Information Security Management is equal to

1.148 +.538 (Communication and Operation Management). Participants' organization Information Security Management increases .538 for each 1 present increase of Communication and Operation Management. Therefore, H8 is accepted.

Table 32. *Multiple Regression Analysis.*

Hypotheses	Unstandardized Coefficients		standardized Coefficients	t-value	F	Significance	Hypotheses Status
	β	Std. Error	(Beta)				
H1	.584	.114	.387	5.102	26.028	.000	Accepted
H2	.674	.070	.619	9.581	91.798	.000	Accepted
H3	.387	.088	.341	4.409	19.442	.000	Accepted
H4	.135	.103	.108	1.316	1.732	.190	Rejected
H5	.574	.109	.396	5.249	27.551	.000	Accepted
H6	.039	.088	.036	.444	.197	.658	Rejected
H7	.095	.105	.075	.912	.831	.363	Rejected
H8	.538	.133	.315	4.033	16.265	.000	Accepted

4.5. Final Fit Model

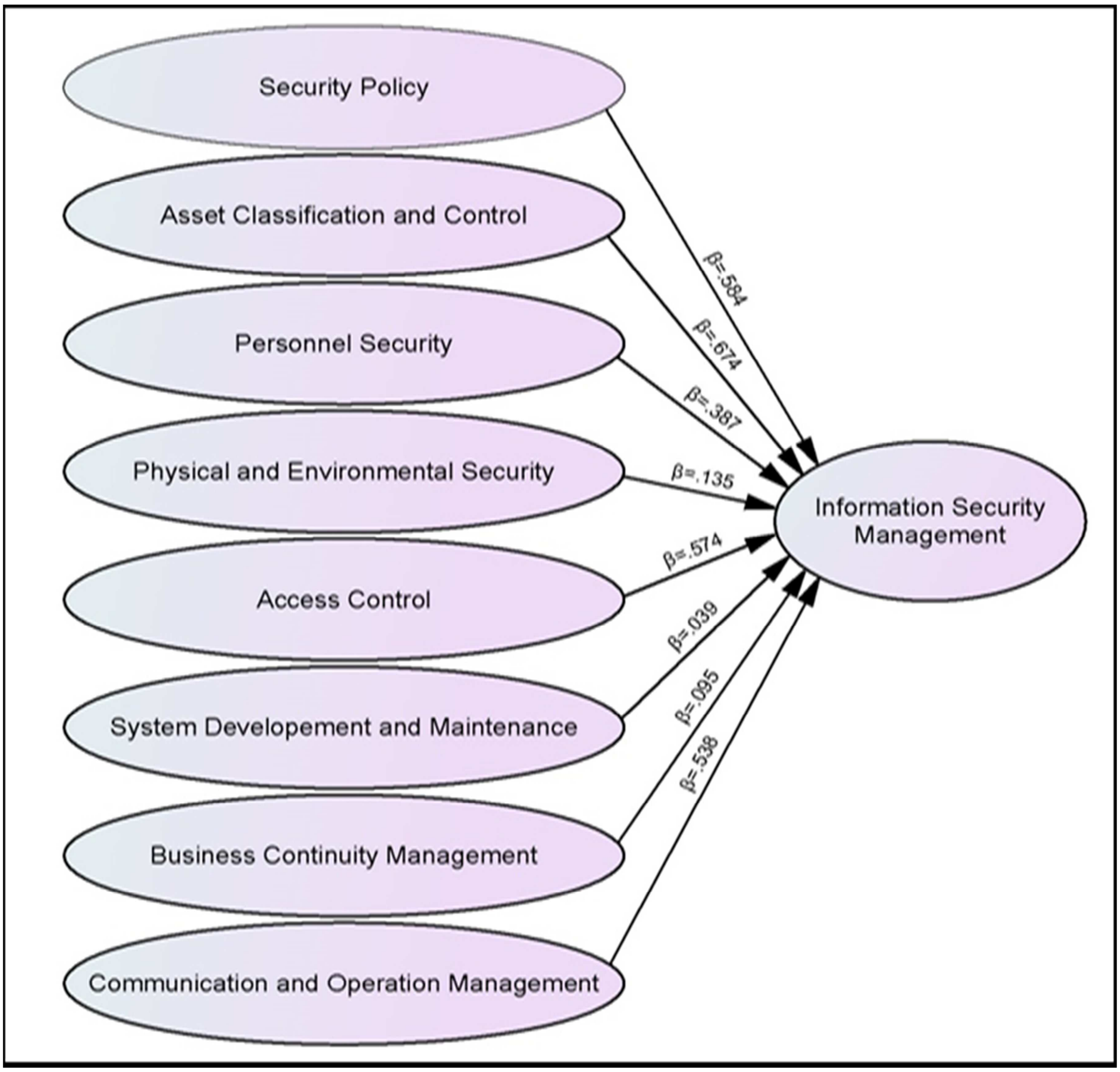
Security Policy
Asset Classification and Control
Personnel Security
Physical and Environmental Security
Access Control
System Developement and Maintenance
Business Continuity Management
Communication and Operation Management
Information Security Management
β=.584
β=.674
β=.387
β=.135
β=.574
β=.039
β=.095
β=.538

Figure 3. *Final Fit Model.*

4.6. IS Managers Awareness Towards Information Security Standards

We have asked the IT managers to state their awareness towards different information security standards such as SABS ISO/IEC 17799 (Part 1), SABS 7799 (Part 2), and RFC 21966: Site Security Handbook.

It is shown in Figure below, 70% of respondents are not aware of any information security standards, while only 30% of them had heard of at least one information security standards.

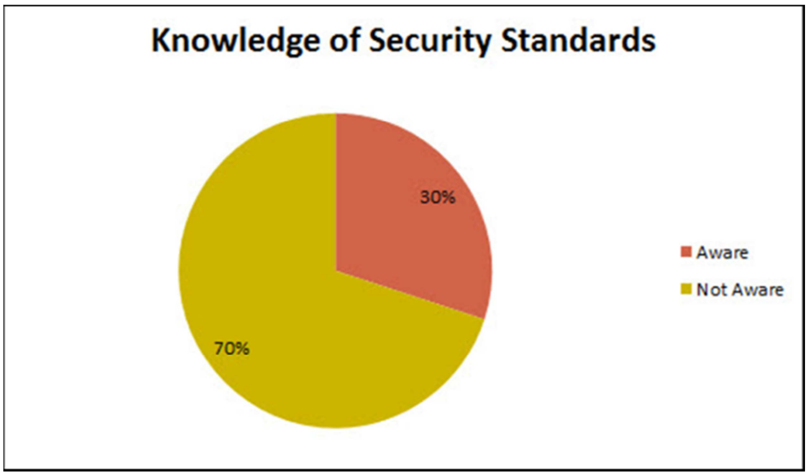

Figure 4. *IS Managers Awareness.*

It is concluded that most of the IT managers in the participating organizations are not adequately involved in information system standards. Thus they are not able to implement the standards in their companies as well for several reasons among which is they never heard of such standards.

4.7. Information Security Breach

We have asked IT managers about the occurrences of security breaches to indicate whether their companies have suffered from which kind of information security breach if any. The result is shown in the table below indicates that only 36% of companies have not suffered from any security breaches while the majorities have suffered from various types of security breaches

Table 33. *ISM Breach.*

The occurrence of a Security Breach	Frequency	%
Occurred	96	64
Did not Occur	54	36
Total	150	100

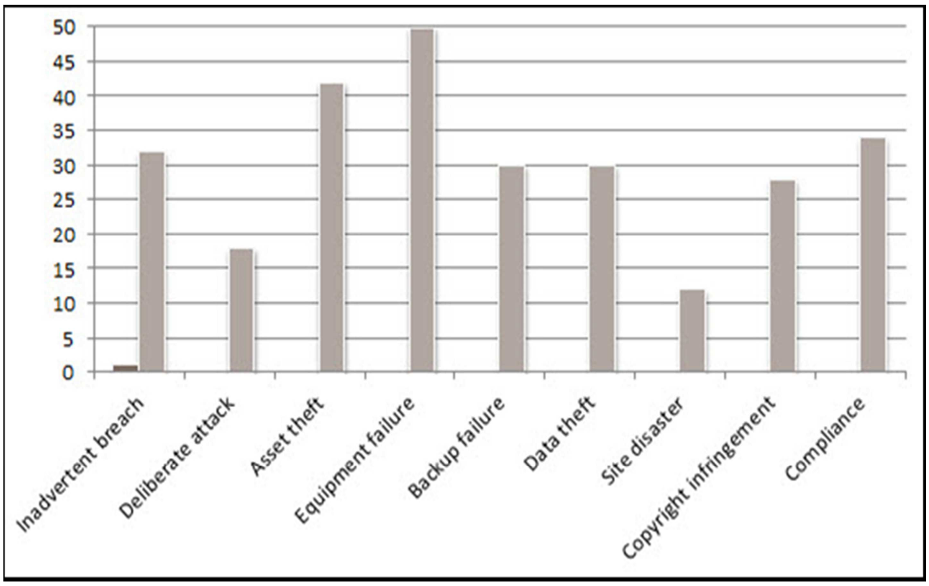

Figure 5. *Information Security Breach Types Grap.*

5. Conclusions and Recommendations

It has been known for a long time that Majority of organizations relations with IS are not sufficient, this might be understood from the lack of IS consultations within or outside the organization. However, Companies moderately pay attention to the issues of systems development and maintenance, business continuity management, physical and environmental security, asset classification and control.

Companies do not attribute sufficient value to other subjects like proper security policy, access control, communications and operation management, personnel security and organizational security. The importance of these issues must be explained to the companies especially IT managers, along with the costs and reasons for the problems it can cause. This will allow them to have better practices with sufficient resources as well as maintaining their information security. Therefore, it is recommended to follow the following recommendations for each component of information security:

Security Policy - Managers should involve employees in the process of generating the policies. In addition, it is recommended to organizations to use template documents which are available online in order to construct information security policies and also to enhance the managers understanding to address the policies in proper means according to their businesses.

Asset Classification and Control - As asset classification and control is a significant topic for organizations, the managers should make their staff aware of controlling local and remote access to their information assets adequately. In addition, staff must know what to do with information with regard to its consequences of abuse usage as well as storage, archiving, backup and destruction.

Personnel Security - Companies must ensure that employees are appropriately trained and stay alert in respect to information security. Staff must realize that information security is not an alternative, but it is a legal, ethical as well as an operational requirement that could determine the difference between business continuance and failure.

Physical and Environmental Security - The company must assure that staffs that travel with portable computers are aware of the risk relating to theft and the potential liability through comprised data. Moreover, companies should be aware of visitors who are visiting their premises. Visitors should not be left to wander around on their own. Furthermore, servers must be maintained in air-conditioned, fire-retardant, power conditioned secure facilities.

Communications and Operations Management - Companies must make use of a firewall within the company as well as with service provider or public networks. They have to update their anti-viruses protection regularly and in the event of security incidents, they can protect systems as best as it is possible. It is recommended to IT managers to implement file server operating systems in order to provide centralized user accounts as well as password management, policy controls both.

Access Control - Companies must implement a Network Server Operating System. Once installed, access to system and data is not possible without valid user accounts and passwords. Password policies can be set, enforcing password changes frequency and password criteria and complexity, such as minimum length and special characters. Besides, most of these systems provide comprehensive auditing facilities whereby log files indicate: the identity and time that users have logged on and off, what directories and folders have been accessed and more importantly, what attempts have been made to access directories and folders that users do not have rights to.

System development and maintenance - Organizations must provide auditing of its resources and data and this auditing must be always updated in order to monitor and identify data types along with keeping track of the organization system and all its related tasks, information, and support.

Business Continuity Management - Business Continuity Management is a governance task. Not only having someone who is a candidate to become responsible to manage the business continuity plan, but you also cannot assign such position to normal candidates rather you should look for most suitable personnel for this task considering things like experience and knowledge background related to security. In addition, organizations need to design a business continuity management plan and revise it annually. The complexity of the plan depends on the size of the organization. Furthermore, the business continuity plan has to be realistic and practical to become successfully implemented. Some questions must be answered such as:

1. What will happen if key personnel quit the job or passed away?
2. What will happen if possible loss of business data and systems occur?
3. What are the financial implications of a disaster?
4. What about outsourcing risk, such as insurance?
5. What are the legal implications of lost data?

Suggestion for Future Research

As Academicians and knowledge seekers we would strongly suggest that researchers interested in security awareness studies to replicate this study among various industries and different countries, we also suggest that the questionnaire could be modified with extra questions to open the door for new concept of findings like social-cultural differences, different people preservations and their correlations with information security management, and other interesting domains to get a whole new different result and findings. In the end, we also would like this study to be conducted among information security students in universities to widen their security perceptions and enable them to become better security personnel when they go to the industry.

References

[1] Kruger, H., and Kearney, W. (2006), A prototype for assessing information security awareness, Computers & Security, 25 (4), pp. 289-296.

[2] Flowerday, S., and Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. Computers & Security, 61, pp. 169-183.

[3] Kritzinger, E. and Smith, E. (2008). Information security management: An information security retrieval and awareness model for the industry. Computers & Security, 27 (5-6), pp. 224-231.

[4] Blakley, B., McDermott, E., and Geer, D. (2001). Information security is information risk management. Proceedings of the 2001 workshop on new security paradigms - NSPW '01.

[5] Go-gulf. (2016). Social Media in Saudi Arabia - Statistics and Trends. [online] Available at: http://www.go-gulf.com/blog/social-media-saudi-arabia/ [Accessed 2 Feb. 2017].

[6] Global Media Insight. (2016). Saudi Arabia Social Media Statistics 2016 - Official GMI Blog. [online] Available at: http://www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics/ [Accessed 2 Feb. 2017].

[7] National Transformation Program 2020. (2016). pp. 32-33.

[8] Dhillon, G. and Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. Communications of the ACM, 43 (7), pp. 125-128.

[9] Eminağaoğlu, M., Uçar, E. and Eren, Ş. (2009). The positive outcomes of information security awareness training in companies – A case study. Information Security Technical Report, 14 (4), pp. 223-229.

[10] Raymond, L. (1990). Organizational context and information systems success: A contingency approach. Journal of Management Information Systems, 6 (4), 5-20.

[11] Dutta, A. and McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. California Management Review, 45 (1), pp. 67-87.

[12] Alsaif, M., Aljaafari, N. and Khan, A. (2015). Information Security Management in Saudi Arabian Organizations. Procedia Computer Science, 56, pp. 213-216.

[13] Frühwirth, C. (2009). On Business-Driven IT Security Management and Mismatches between Security Requirements in Firms, Industry Standards, and Research Work. Lecture Notes in Business Information Processing, pp. 375-385.

[14] Peltier, T. (2005). Information security risk analysis. 2nd ed. Boca Raton: Auerbach Publications.

[15] Taylor, A. (2008). Information Security Management Principle. 1st ed. Swindon: The British Computer Society.

[16] Safa, N. and Von Solms, R. (2016). An information security knowledge sharing model in organizations.

[17] Sameera Mubarak, (2016), "Developing a theory-based information security management framework for human service organizations", Journal of Information, Communication, and Ethics in Society, Vol. 14 Iss 3 pp.

[18] Järveläinen, J. (2012). Information security and business continuity management in inter-organizational IT relationships. Information Management & Computer Security, 20 (5), pp. 332-349.

[19] Abhishek Narain Singh M. P. Gupta Amitabh Ojha, (2014), "Identifying factors of “organizational information security management”, Journal of Enterprise Information Management, Vol. 27 Iss 5 pp. 644-667.

[20] Chander, M., Jain, S. and Shankar, R. (2013). Modeling of information security management parameters in Indian organizations using ISM and MICMAC approach. Journal of Modeling in Management, 8 (2), pp. 171-189.

[21] Li-Hsing Ho Ming-Tsai Hsu Tieh-Min Yen, (2015), "Identifying core control items of information security management and improvement strategies by applying fuzzy DEMATEL", Information &Computer Security, Vol. 23 Issue 2 pp. 161-177.

[22] Alavi, R., Islam, S. and Mouratidis, H. (2016). An information security risk-driven investment model for analyzing human factors.

[23] Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C. and Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. Procedia - Social and Behavioral Sciences, 147, pp. 424-428.

[24] Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not.

[25] European Network and Security Agency, (2007). Information security awareness initiatives Current practice and the measurement of success. [online] Available at: http://intug.org/2007/08/enisa-presents-report-on-information-security-awareness/ [Accessed 27 Feb. 2017].

[26] Hansche, S. 2001, designing a security awareness program: part 1, Information Systems Security, January/February, pp. 14-22.

[27] Finextra. UK phishing fraud losses double. Available from: <http://www.finextra.com/fullstory.asp?id¼15013>; 2006 [accessed February 2017].

[28] Cone, B., Irvine, C., Thompson, M. and Nguyen, T. (2007). A video game for cybersecurity training and awareness. Computers & Security, 26 (1), pp. 63-72.

[29] Ahlan, A., Lubis, M., and Lubis, A. (2015). Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. Procedia Computer Science, 72, pp. 361-373.

[30] Ahlan, A. and Lubis, M. (2011). Information security awareness in university: Maintaining learnability, performance, and adaptability through roles of responsibility. 2011 7th International Conference on Information Assurance and Security (IAS).

[31] Tsohou, A., Karyda, M., Kokolakis, S. and Kiountouzis, E. (2012). Analyzing the trajectories of information security awareness.

[32] Ki-Aries, D., Faily, S. and Beckers, K. (2016). Persona-Driven Information Security Awareness. [online] Bournemouth, BISL. Available at: http://eprints.bournemouth.ac.uk/23808/1/kifa16.pdf [Accessed 27 Mar. 2017].

[33] Alarifi, A., Tootell, H. and Hyland, P. (2012). A study of information security awareness and practices in Saudi Arabia. 2012 International Conference on Communications and Information Technology (ICCIT).

[34] Ngoqo, B. and Flowerday, S. (2015). Exploring the relationship between student mobile information security awareness and behavioral intent.