Information security practice in Saudi Arabia: case study on Saudi organizations

Zakarya A. Alzamil
Software Engineering Department, King Saud University, Riyadh, Saudi Arabia

Received 13 January 2018
Revised 6 March 2018
21 April 2018
5 June 2018
Accepted 6 June 2018

Abstract

Purpose – Information security of an organization is influenced by the deployed policy and procedures. Information security policy reflects the organization's attitude to the protection of its information assets. The purpose of this paper is to investigate the status of the information security policy at a subset of Saudi's organizations by understanding the perceptions of their information technology's employees.

Design/methodology/approach – A descriptive and statistical approach has been used to describe the collected data and characteristics of the IT employees and managers to understand the information security policy at the surveyed organizations. The author believes that understanding the IT employees' views gives a better understanding of the organization's status of information security policy.

Findings – It has been found that most of the surveyed organizations have established information security policy and deployed fair technology; however, many of such policies are not enforced and publicized effectively and efficiently which degraded the deployed technology for such protection. In addition, the clarity and the comprehensibility of such policies are questionable as indicated by most of the IT employees' responses. A comparison with similar studies at Middle Eastern and European countries has shown similar findings and shares the same concerns.

Originality/value – The findings of this research suggest that the Saudi Communications and Information Technology Commission should develop a national framework for information security to guide the governmental and non-governmental organizations as well as the information security practitioners on the good information security practices in terms of policy and procedures to help the organizations to avoid any vulnerability that may lead to violations on the security of their information.

Keywords Information security, Case study, Information security policy,
Information security in Saudi Arabia, Information security management, Information security procedures

Paper type Research paper

1. Introduction

Information security has been recognized by most organizations worldwide as an important aspect of asset protection. However, despite such recognition, many organizations lack information security policy or its enforcement. Many reported incidents have occurred as a result of security vulnerabilities which are influenced by human behaviors and attitudes, or because of the lack of written formal policy for information security (Colwill, 2009; DCMS, 2016). Information security surveys have indicated that security threats are increasing over the years, and the most common vulnerabilities are internal to organizations; for example, the continued tendency of employees to open malicious emails and click on attachments or links (DCMS, 2016).

Although there are no statistical studies that reveal security breaches and incidents in Saudi Arabia, information security threats are increasing, and they have occurred at many levels. Among the most important attempts to breach security at government agencies were the attacks on 30,000 workstations at Saudi Aramco that attempted to stop oil production

Information & Computer Security
Vol. 26 No. 5, 2018
pp. 568-583

2056-4961
DOI 10.1108/ICS-01-2018-0006

(The New York Times, 2012), and an attempted attack on the Saudi Arabian Ministry of Foreign Affairs that was carried out in 2015 (MOFA, 2015). The Saudi Government has recognized the importance of information security regulations, as a result of which two important laws have been declared: the information technology criminal law and the electronic transaction law (MCIT, 2017). The information technology criminal law aims to combat cybercrimes by identifying them and determining their punishments to enhance information security. The electronic transaction law aims to control, regulate and provide a legal framework for electronic transactions and signatures.

Despite the governmental efforts to address information security issues, the status of information security within the public and private Saudi organizations is not well investigated. Therefore, such a study is very important in understanding the state of information security practices within Saudi organizations.

The author has conducted a research study that investigated the information security practices at a subset of Saudi organizations. In this research study, the author has developed a set of research questions related to information security practices, in which answering them may help to better understand current information security practices in Saudi Arabian organizations.

The aim of this paper is to investigate the status of the information security policy at a subset of public and private organizations in Saudi Arabia by understanding the perceptions of their IT employees and managers. Therefore, the following two research questions have been developed, which the author attempts to answer within this article:

RQ1. To what extent are the policies and procedures used suitable for ensuring information security?

RQ2. To what extent are the technologies deployed suitable to ensure information security?

This paper is organized as follows: next section presents the related work, then the research methodology and study tool are described, after that, the results are discussed, then the research findings related to this study are presented, and the conclusions are presented in the last section.

2. Related work

There are many studies that have investigated the influence of human aspects on information security based on human behavior in different countries, e.g. Norway (Albrechtsen, 2007), UK (DCMS, 2016), China (Huang *et al.*, 2011) and Finland (Vance *et al.*, 2012). These studies have investigated different approaches and techniques to better understand the impacts of human behaviors on information security.

In addition, there are many studies that have investigated the implementation of information security policy and procedures. An early attempt to implement an information security policy within the health care environment in UK is presented in Gaunt (1998). This combined risk analysis with surveys of users, in which the role and responsibilities for information security were defined along with the appropriate structure and process for installing an information security policy with consideration of the human factors in the health-care environment. An information security policy development life cycle (ISPDLC) has been proposed in Flowerday and Tuyikeze (2016) to provide a framework for developing and implementing an effective information security policy. The proposed framework is constructed using a formal analysis of information security policy development methods,

and validated and refined by surveying 310 security professionals. In Knapp *et al.* (2009), an information security policy process model has been proposed, by surveying 220 certified information system security professionals from different countries, that reflects the recommended practices of the professionals surveyed. A study that examined enterprise information security policy of 97 small and medium-sized enterprises in Turkey has been presented in Yildirim *et al.* (2011). In Ku *et al.* (2009), the current status of information security policy of the Taiwanese Government along with an example of governmental institutions that self-adopted the information security management system (ISMS) has been presented as a pilot study of ISMS self-implementation that can serve as guidance for those organizations that are going to implement ISMS by themselves.

There have been a small number of studies that investigated information security practices within Saudi Arabian organizations. For instance, a study was performed to investigate the security threats of the computerized accounting information systems in Saudi organizations (Abu-Musa, 2006). Another study (Abu-Musa, 2010) aims at examining the existence and implementation of information security governance in Saudi organizations. A research study has been performed in Alageel (2003) that aims to develop an information security awareness and training program for the employees of the Royal Saudi Naval Forces based on selected information security courses provided by four training institutes in the USA. Another study Alarifi *et al.* (2012) has examined the level of information security awareness among the general public in Saudi Arabia to understand the relationship between high risk level and information security awareness in Saudi Arabia. A research study has been performed in Alnatheer and Nelson (2009) that aims to identify the important conditions for creating an information security culture in Saudi organizations. A conceptual framework has been used in Alfawaz (2011) to understand the relationships of the national, organizational and technological values and their impact on the development and deployment of information security culture in Saudi Arabia.

Although these studies have investigated the information security management issues related to awareness, cultures and regulations; the status of the information security policy within Saudi public and private organizations was not investigated. Therefore, this study aims to conduct such investigation to better understand the practices of information security in terms of policy and procedures within public and private organizations in Saudi Arabia.

3. Methodology and study tool

The author has used a descriptive and statistical approach to data gathered from IT employees and managers to understand approaches to information security policy in those organizations surveyed. This type of research methodology is used to describe the state of the information security practices at these organizations rather than judging or interpreting such practices. The research study was conducted as follows; first the study questions were developed, then the case study was identified in which the study samples were selected; next the survey questionnaires were designed, and then the questionnaires were distributed and data were collected; after that the data were processed and manipulated using the statistical tool SPSS; finally, the data were analyzed and interpreted.

This study is divided into two parts. The first investigates perceptions of IT employees to information security practices. The second investigates the same perceptions in IT managers. Such a qualitative approach requires the use of surveys. The author has therefore developed two questionnaires that function as a research tool to investigate the study questions. The first, for IT employees, consists of 25 statements. The second, for IT managers, consists of 39 statements. In relation to each of the statements, respondents were asked to indicate whether they agreed, disagreed or were uncertain about compliance within

their organization. As the most of the target study samples are native Arabic speaking employees and managers, the questionnaires were, originally, written in the Arabic language and their statements were simplified to assure their clarity and understandability. In addition, the questionnaires were translated to the English language for the non-Arabic speaking employees and managers. The statements in the questionnaires were designed to cover the study's questions that are based on the four components of the information security business model (policy, awareness, training and education and technology) which was introduced by the National Institute of Standards and Technology NIST (Wilson and Hash, 2003). Some of the statements were based on the ISO/IEC 17799-2005[1] Information Security Audit Tool, and some others were designed to cover some local cultural issues that may influence information security.

Appendices 1 and 2 provide complete list of the two questionnaires' statements. The statements in the questionnaires cover many information security aspects such as the security controls related to human behaviors and awareness (e.g. S12-S19, and S21 for employees; S35 for managers) and policy enforcement (e.g. S1-S6, and S20 for employees; S1-S19 for managers), as well as information security related to training and education (e.g. S7-S8 for employees; S20-S21 for managers). In addition, the statements in the questionnaires investigate the deployed information security technology (e.g. S9-S11 for employees; S22-S34 for managers). The questionnaires were designed to measure the respondents' knowledge, behavior and attitude toward information security practices related to information security policy and procedures rather than identifying or evaluating the effectiveness of such practices and/or deployed technologies.

Although the author has investigated only the IT employees and managers rather than other employees at these organizations, the author believes that, understanding the information security practices of the IT employees and managers gives a better understanding of the state of information security of the entire organization. The author considers this to be a credible hypothesis because IT employees have greater access to the organization's critical business data assets. IT employees and managers can therefore be expected to have received better training in information security and to have a greater understanding and awareness of good information security practices. Also, most the IT employees are likely to be specialized in one of the information technology or related fields as a result of obtaining a degree or certification in which they gain knowledge and skills that may contribute to good information security practices. Although the information security practices of IT employees do not necessarily represent information security practices followed by the other employees of the organization; it is likely that poor practices by IT employees and managers will be reflected in the organization as a whole and vice versa. In addition, IT employees are most likely to understand information security aspects to assure a better interpretation of their responses to the questionnaires' statements. The author has selected the perceptions of the IT employees and managers as a measure to understand the status of information security practices because most of the issues related to information security are an attitude and behavior, or related to them, which cannot be measured by the standard metrics.

The research surveyed employees and managers of IT departments in both public and private sector organizations. These included banks, insurance companies, IT companies, hospitals, industrial companies, educational institutions, military and government agencies. The feedback was collected from 69 employees and 65 managers, with the total of 134 respondents covering 41 organizations (14 public and 27 private). The collected study data were processed using the SPSS software, presented using a descriptive quantitative approach and then the statistical results were analyzed to draw the research findings.

Table I shows the demographic properties of the study samples. It should be noted that, for the purposes of simplifying the analysis, the demographic in both the IT employees and

Property/value	Employees Frequency	(%)	Managers Frequency	(%)
Qualification				
PhD/MSc	4	5.8	17	26.1
BSc	42	60.9	41	63.1
Diploma	23	33.3	4	6.2
Unspecified	0	0	3	4.6
Specialty				
Computer	52	75.4	43	66.2
Engineering	8	11.6	14	21.5
Management	5	7.2	4	6.1
Others	4	5.8	2	3.1
Unspecified	0	0	2	3.1
Experience				
>10 years	13	18.8	27	41.5
5-10 years	17	24.6	25	38.5
1-4 years	34	49.3	10	15.4
<1 year	1	1.4	N/A	N/A
Unspecified	4	5.8	3	4.6
Sector				
Government	25	36.2	24	36.9
Private	41	59.4	38	58.5
Unspecified	3	4.3	3	4.6
Nature of job				
Dept. Director	9	13	N/A	N/A
Employee	14	20.3	N/A	N/A
Developer	19	27.5	N/A	N/A
Sys. Analyst/Designer	22	31.9	N/A	N/A
Unspecified	5	7.2	N/A	N/A
Total		69		65

Table I.
Property of the surveyed employees and managers

managers groups was divided into two broad educational categories (Diploma and BSc) and into two specialty groups (Computer and Other).

To provide assurance that the statements in the questionnaires correlate with the study questions, the correlation co-efficient between each of the two research questions and its related statements was calculated. The results are shown in Table II. This demonstrates that there is a good correlation between the statements in the questionnaires and their respective research questions.

To provide assurance that each of the research questions is measured by the related statements in the questionnaires, a Cronbach's alpha test was used. Table III shows the value of Cronbach's alpha for the study questions in relation to the questionnaires. The

Question	Employees' statements Correlation coefficient	No. of statements	Managers' statements Correlation coefficient	No. of statements
Q1	0.44	7	0.93	19
Q2	0.56	3	0.87	13

Table II.
Correlation of the study questions to the total score

value of Cronbach's alpha is high enough to indicate that the questionnaire's statements provide effective measurement of the study questions.

Further tests were used to determine the statistical significance of the variability between two or more sample groups. These include analysis of variance (ANOVA), *t*-test, Scheffe test and Chi-square test.

4. Results

This section presents a discussion of the responses from IT employees and managers in relation to the two study questions. Each question is discussed separately below. In addition, comparison of the outcomes of this study with related studies in other countries is provided.

4.1 First question

To what extent are the policies and procedures used suitable for ensuring information security?

In total, 26 statements within the study questionnaire relate to this question. Seven of these questions were put to IT employees and 19 to Managers. Tables IV and V show the responses of IT employees and managers, respectively, to these statements.

Statistical tests were carried out on the responses shown in Table IV. These show no significant variations between employees responses based on the nature of their job, their qualifications, their experience or the sector within which they work.

As can be seen from Table IV, 58 per cent of respondents agree that there are procedures and penalties to assure the information security of their organization; 43.5 per cent agree

Table III.
Values of Cronbach's alpha for the study's questions

Questionnaires	No. of statements	Alpha's value
Employees	25	0.26
Managers	39	0.91

Table IV.
Employees' response to statements related to Question 1

No.	Statement	Agree (%)	Maybe (%)	Disagree (%)	No answer (%)
S1	We are not allowed to carry in/out CD, DVD, USB storage devices to/from computing center	43.5	29	27.5	0
S2	Because of the trust among the employees and the management, I can carry in storage devices into the computing center	37.8	21.7	39.1	1.4
S3	There are procedures and penalties to assure the information security	58	24.6	16	1.4
S4	The information security procedures are not clear	37.7	31.9	30.4	0
S5	Non-employees are not allowed to enter into computing center	65.2	18.8	16	0
S6	Other employees from other departments, freely, visit me at the computing center	17.4	27.5	55.1	0
S20	I feel that the management exaggerates on the issue of information security in terms of the procedures and used technology	20.3	21.7	58	0

No.	Statement	Agree (%)	Maybe (%)	Disagree (%)	No answer (%)
S1	We have policy and procedures that control the daily business to assure information security	78.5	21.5	0	0
S2	We have/plan to have international certification (e.g., ISO27001/BS-7799) to assure the quality of information security process	44.6	26.2	27.7	1.5
S3	When designing and building the software systems, information security is considered as one of the major issues of system design and development	78.5	20	1.5	0
S4	The information security procedures are written and available to all employees to follow	49.2	43.1	7.7	0
S5	We have an information security technical plan (quarterly, half yearly, yearly) that we implement and follow	47.7	33.8	18.5	0
S6	Information security procedures are clear and understandable for all employees	52.3	40	7.7	0
S7	All employees are required to consent for the information security policy and procedures	52.3	24.6	23.1	0
S8	Employees are not permitted to bring storage devices (USB flash, CD, DVD, etc.) into the computing center	38.5	26.2	35.3	0
S9	Employees are not permitted to move storage devices out of the computing center	41.5	27.7	30.8	0
S10	Non-authorized employees are strictly not permitted to enter the computing center	63.1	27.7	9.2	0
S11	Information security experts are available at the computing center	55.4	33.8	10.8	0
S12	We have an emergency plan and clear procedures to follow in case of any emergency or threats to occur	52.3	40	7.7	0
S13	The computer machines are frequently examined to recycle the outdated ones in a way that assures the security of the confidential information	61.5	27.7	10.8	0
S14	We have technical procedures to follow by the employees to update their computer machines for any security vulnerability	57	33.8	9.2	0
S15	We have an information classification scheme to distinguish the confidential information from the public ones	50.8	32.3	13.8	3.1
S16	We apply precise procedures for the employees' recruitment to work with confidential/sensitive information	44.6	32.4	21.5	1.5
S17	We assure that the employees understand their duties before appointing them to prevent any misuse of the computing center's resources and/or possible deliberate act of theft	52.3	40	6.2	1.5
S18	We have procedures for contractors' access to the computing center to assure the information security	70.8	18.5	10.7	0
S19	We monitor the employees' commitment to the policy that obligates them to update their computer machines against any security vulnerability	58.5	36.9	4.6	0

Table V.
Managers' response to statements related to Question 1

that they are not allowed to carry storage devices in or out of their computing center; and 55.1 per cent disagree that other staff are free to visit the computer center. These answers appear to indicate a reasonable degree of policy and procedural assurance for information security. Furthermore, it seems evident that the majority of employees (58 per cent) feel that

the organization is not exaggerating the issue of information security in terms of policy, procedure and technology; and thus that a good information security approach is normal. However, some of the other responses shown in Table IV raise some concerns. For example, more than two-thirds of respondents felt that information security procedures in their organization are not clear. Moreover, more than one third of respondents felt that employees are able to violate information security policy and procedures because their manager trusts them. In addition, in the case of a number of responses (i.e. S1, S2, S3, S4, S5, S6 and S20), 20-30 per cent of respondents either disagree with, or are not sure of, the enforcement of policy and procedure. Such responses indicate potential problems with information security communication, training or enforcement. Use of the "may be" response tends to indicate that a number of respondents feel that information security policy and procedure is present but not enforced.

Table V shows manager's responses to the statements related to the first research study question. Again, statistical analysis shows no significant variability between managers' responses based on their qualifications, their specialty, their experience or the sector within which they work.

As can be seen from Table V, in 13 of the 19 statements relating to information security policy and procedure, more than 50 per cent of respondents agreed with positive statements. These responses are encouraging with respect to compliance with good practice.

However, responses to a number of the statements (S4, S6, S8, S9, S12 and S17) may indicate a lack of policy and procedure enforcement and/or poor understanding of policy and procedure on the part of those who are required to implement them.

4.2 Second question

To what extent are the technologies deployed suitable to ensure information security?

In total, 16 statements within the study questionnaire relate to this question. Three of these statements were put to IT employees and 13 to managers. Tables VI and VII show the responses of IT employees and managers, respectively, to these statements.

Statistical tests were carried out on the responses shown in Table VI. These show no significant variations between employees' responses based on the nature of their job, their qualifications, their experience or the sector within which they work.

As can be seen from Table VI, 71 per cent of respondents agree that the provided software and hardware technologies are suitable for assuring information security; 72.5 per cent agree that there are regular software updates for their computers to cover any security vulnerability; and 65.3 per cent agree that there is a regular technical support to maintain the management of security vulnerability. These answers appear to indicate a reasonable degree of suitability of the deployed technology to ensure information security.

No.	Statement	Agree (%)	Maybe (%)	Disagree (%)	No answer (%)
S9	Computing center provides suitable technologies (software/hardware) to assure information security	71	21.8	5.8	1.4
S10	My desktop computer is updated on regular basis to cover any security vulnerability	72.5	18.8	8.7	0
S11	Technical support is available on regular basis to maintain any security vulnerability	65.3	27.5	7.2	0

Table VI. Employees' response to statements related to Question 2

No.	Statement	Agree (%)	Maybe (%)	Disagree (%)	No answer (%)
S22	We schedule the operating systems' updates for the servers and employees desktops on regular basis to block any security vulnerability	70.8	24.6	4.6	0
S23	We scan the storage devices, such as CD, DVD, USB, for any viruses before being used at the computing center	61.5	20	17	1.5
S24	We update the anti-virus and anti-spam software on regular basis	78.5	18.5	3	0
S25	We use access control tools to access sensitive locations and computer machines (e.g. fingertip, password, magnetic card, etc.)	67.7	23.1	9.2	0
S26	We use hardware protection systems (anti-fire, backup protection, etc.)	73.8	23.1	3.1	0
S27	We use cooling, heating, and ventilation systems to assure the safety of the data storage devices	84.6	10.8	1.5	3.1
S28	Employees are not permitted to install any software into their desktop computers without the permission of the system administrator	53.8	30.8	15.4	0
S29	We have backup systems for electrical power and communication in case of electrical/communication failure	75.4	13.8	10.8	0
S30	We have data backup procedure that is performed on daily/weekly/monthly/yearly basis	87.7	7.7	4.6	0
S31	We have protection systems such as hardware/software firewall, IDS systems, etc.	83.1	9.2	7.7	0
S32	We have cryptography systems (e.g. encryption-based solutions)	55.4	26.1	18.5	0
S33	We apply content filters on incoming Web requests	55.4	26.2	13.8	4.6
S34	We have scanning and analysis tools to detect spying programs	64.6	26.2	9.2	0

Table VII.
Managers' response to statements related to Question 2

Table VII shows manager's responses to the statements related to the second research study question. Again, statistical analysis shows no significant variability between managers' responses based on their qualifications, their specialty or the sector within which they work. However, significant difference between managers' responses based on their experience has been found by one-way ANOVA test ("f" test) with significance at 0.01. The Scheffe test has identified the variation for the favor of the first group (more than 10 years of experience), which indicates that managers with longer experience are more active in responding to this question of the study than others with less experience.

As can be seen from Table VII, 65 per cent or more of respondents agreed with positive statements for 9 out of 13 statements relating to suitability of the deployed technology, and 54 per cent or more agreed with the remaining four statements. These responses are encouraging with respect to suitability of the deployed technology for information security assurance.

However, responses to a number of the statements (e.g. S22, S23, S25, S26, S28, S32, S33 and S34), in which 20 per cent or more are not sure of such deployment or practice, indicate some concerns about the efficiency of deployed technologies that may be degraded by the lack of policy enforcement.

4.3 Results' comparison

To have a better view of the results of this study, we compare the achieved results with similar information security practices at other countries. We have chosen two counties, one Middle Eastern country, namely, Turkey (Yildirim *et al.*, 2011), that shares some common culture, and another Western country, namely, UK (DCMS, 2016), that has a different culture. The first survey (Yildirim *et al.*, 2011) examined 97 small and medium-sized Turkish enterprises, and the second survey (DCMS, 2016) examined 1,008 UK businesses. Table VIII compares the results of this study in 14 security practice areas with similar studies in the same areas within Turkey and the UK. N/A is used in Table VIII to indicate where similar security practice areas could not be found in the two studies used for comparison.

Although we observed some concerns as stated earlier, it is interesting to find much similarity of information security practices between Saudi Arabia and Turkey for most of the practices. For the comparison with UK, the results of some practices, e.g. anti-virus and anti-spam updates, availability of protection systems, and using access control solutions, are close to achieved results in Saudi Arabia. However, as can be seen, the result of the information security practices in UK for the items 1, 2, 3, 4, 5, 7 and 13, are very low comparing to Turkey and Saudi Arabia. It should be noticed that, unlike the UK survey (DCMS, 2016); the responses in the Turkish survey (Yildirim *et al.*, 2011) and in this study

No.	Security practice/issue	Saudi Arabia (%)	Turkey (%)	UK
1	Have a written information security procedures	49.2	77	15%-73% with average of 29%
2	Have procedures for contractors' access to the computing center/information systems	70.8	84.5	25%-34% with average of 13%
3	Are aware of information security standards e.g. ISO27001	44.6	31	13%-60% with average of 18%
4	Have an emergency plan/incident management processes	52.3	64.9	6%-42% with average of 10%
5	Have clear and understandable Information security policy	52.3	85	N/A
6	Have an information classification scheme for data	50.8	N/A	58% for large organizations with average of 46%
7	Have information security experts	55.4	60.8	60%-75% with average of 34%
8	Have procedures and penalties to assure the information security	58	55.7	N/A
9	Have backup systems in case of electrical/communication failure	75.4	77.4	N/A
10	Have scheduled software updates on regular basis	70.8	75.2	88%
11	Have anti-virus and anti-spam software updates on regular basis	78.5	86.6	83%
12	Have protection systems such as firewall and IDS systems	83.1	71.2	85%
13	Have cryptography systems (e.g. encryption-based solutions)	55.4	N/A	34%
14	Have access control solutions for sensitive locations (e.g. fingertip, password, magnetic card, etc.)	67.7	N/A	62%

Table VIII.
Comparison of study results with similar surveys

are collected from IT professionals. In addition, about 28 per cent of the UK businesses surveyed (DCMS, 2016) are micro businesses that have very limited information security practices which influences the final findings of that study.

Such comparison has shown similar findings and shares the same concerns in which the state of the current information security practices in Saudi Arabia is similar to, or within the range of, the regional and worldwide information security practices. In addition, the information security concerns, identified in this study, are shared by other regional and worldwide information security surveys.

5. Research findings

The results of this study have shown that, while IT employees recognize the need for information security, there are potential concerns over their understanding of, and ability to comply with, information security policy and procedure. The findings of this study may be summarized as follows:

- Although, most of the surveyed organizations have established information security policy and procedures, many of these are not enforced and publicized effectively and efficiently.
- Results indicate that the clarity and comprehensibility of many information security policies and procedures may be questionable.
- Results suggest that cultural issues, such as the tendency to place undue reliance on the trustworthiness of individuals, may adversely impact compliance with information security good practice.
- Most of the organizations surveyed have reasonable deployment of information security technologies; however, the effectiveness of this may be degraded by poor policy enforcement.
- Most of those surveyed were aware of the business criticality of good information security.
- Results suggest that lack of perception of the importance of internal threats and vulnerabilities, as opposed to those from external sources, may adversely impact good information security compliance.

6. Conclusion

This paper contains a study of the perception of information security policy, procedure and technology among IT employees and managers in a cross-section of Saudi Arabian organizations. Results show that, while most employees recognize the importance of information security to their business, there may be a lack of compliance with good information security practice as a result of failure to appreciate the importance of internal threats and vulnerabilities.

Most of the organizations surveyed showed a potential lack of effective and efficient enforcement of existing information security policies and procedures; a failure which is likely to be common in organizations worldwide (Vance *et al.*, 2012). Such a lack has the potential to degrade the effectiveness of deployed information security technologies. As a consequence, this study suggests that the management of organizations should, as a matter of urgency, establish information security training and awareness programs and should take action to prevent violations of policies and procedures.

Although, the Saudi Communications and Information Technology Commission has developed guidelines for security policies and procedures for government agencies (CITC, 2011), the author recommends that, the CITC should develop a national framework for information security that guides governmental and non-governmental organizations as well as information security practitioners on the good practices in terms of policy and procedures to help avoid vulnerabilities that may lead to information security violations. Such a framework requires collaborative efforts on the part of both governmental and non-governmental agencies and should learn from worldwide good practices.

Although the findings of this research describe the status of the current information security practices in a subset of Saudi organizations, our hypothesis is that understanding the information security practices of the IT employees and managers gives a better understanding of the state of information security of the entire organization. However, investigating the perception of non-IT employees may produce different results, therefore, more studies and investigations are still needed to better understand the information security practices of governmental and non-governmental Saudi organizations, and for comparative purposes. Information security technology is continuously evolving to meet ever-increasing threats, and this requires constant overhaul and updating of security practices. The Government of Saudi Arabia is initiating many projects at all governmental organizations to establish the infrastructure for the e-government, in which the information security is a major component. These projects are likely to influence the issues researched in this study, which indicates the need to provide ongoing monitoring of the effectiveness of information security policy, procedure and technology within Saudi organizations.

Note

1. Now ISO/IEC 27001-2013.

References

Abu-Musa, A. (2006), "Investigating the perceived threats of computerized accounting information systems in developing countries: an empirical study on Saudi organizations", *Journal of the King Saud University*, Vol. 18, pp. 1-26. Computer and Information Sciences.

Abu-Musa, A. (2010), "Information security governance in Saudi organizations: an empirical study", *Information Management and Computer Security*, Vol. 18 No. 4, pp. 226-276.

Alageel, S. (2003), "Development of an information security awareness training program for the royal Saudi naval forces", Master Thesis, Naval Postgraduate School, Monterey, CA.

Alarifi, A., Tootell, H. and Hyland, P. (2012), "A study of information security awareness and practices in Saudi Arabia", *IEEE Proceedings of the International Conference on Communications and Information Technology*, pp. 6-12.

Albrechtsen, E. (2007), "A qualitative study of users' view on information security", *Computers and Security*, Vol. 26 No. 4, pp. 276-289.

Alfawaz, S. (2011), "Information security management: a case study of an information security", PhD Dissertation, Technical Report, Faculty of Science and Technology, Queensland University of Technology.

Alnatheer, M. and Nelson, K. (2009), "Proposed framework for understanding information security culture and practices in the Saudi context", *Proceedings of the 7th Australian Information Security Management Conference*, pp. 6-17.

CITC (2011), "Information security policies and procedures development framework for government agencies", available at: www.citc.gov.sa/ (accessed 23 May 2017).

Colwill, C. (2009), "Human factors in information security: the insider threat: who can you trust these days?", Information Security Technical Report, No. 14, pp. 186-196.

DCMS (2016), "Cyber security breaches survey 2016", Technical Report, Department for Culture Media and Sport.

Flowerday, S. and Tuyikeze, T. (2016), "Information security policy development and implementation: the what, how and who", *Computers and Security*, Vol. 61, pp. 169-183.

Gaunt, N. (1998), "Installing an appropriate information security policy", *International Journal of Medical Informatics*, Vol. 49 No. 1, pp. 131-134.

Huang, D., Raua, P., Salvendy, G., Gao, F. and Zhou, J. (2011), "Factors affecting perception of information security and their impacts on IT adoption and security practices", *International Journal of Human-Computer Studies*, Vol. 69 No. 12, pp. 870-883.

Knapp, K., Morris, R., Marshall, T. and Byrd, T. (2009), "Information security policy: an organizational-level process model", *Computers and Security*, Vol. 28 No. 7, pp. 493-508.

Ku, C., Chang, Y. and Yen, D. (2009), "National information security policy and its implementation: a case study in Taiwan", *Telecommunications Policy*, Vol. 33 No. 7, pp. 371-384.

MCIT (2017), available at:www.mcit.gov.sa/ (accessed 23 May 2017).

MOFA (2015), available at: www.mofa.gov.sa/ServicesAndInformation/news/MinistryNews/Pages/ArticleID201562023465437.aspx (accessed 23 May 2017, in Arabic).

The New York Times (2012), "Aramco says cyberattack was aimed at production", The New York Times, Global business, 10 December, available at: www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0 (accessed on 23 May 2017).

Vance, A., Siponen, M. and Pahnil, S. (2012), "Motivating IS security compliance: insights from habit and protection motivation theory", *Information and Management*, Vol. 49 Nos 3/4, pp. 190-198.

Wilson, M. and Hash, J. (2003), "Building an information technology security awareness and training program", NIST Special Publication 800-50, National Institute of Standards and Technology, US Department of Commerce.

Yildirim, E., Akalp, G., Aytac, S. and Bayram, N. (2011), "Factors influencing information security management in small and medium sized enterprises: a case study from Turkey", *International Journal of Information Management*, Vol. 31 No. 4, pp. 360-365.

Appendix 1

No.	Statement
1	We are not allowed to carry in/out CD, DVD, USB storage device to/from computing center
2	Because of the trust among the employees and the management, I can carry in storage device into the computing center
3	There are procedures and penalties to assure the information security
4	The information security procedures are not clear
5	Non-employees are not allowed to enter into computing center
6	Other employees from other departments, freely, visit me at the computing center
7	Our department, regularly, admits us into training courses in the field of information security
8	I find the effect of the training courses onto my performance in term of information security
9	Computing center provides suitable technologies (software/hardware) to assure information security
10	My desktop computer is updated on regular basis to cover any security vulnerability
11	Technical support is available on regular basis to maintain any security vulnerability
12	I received incoming emails from people I know in which I trust
13	I never open the incoming emails from unknown sender
14	I understand the importance of information security and its impact on my daily business and my organization
15	I always consider information security when performing my daily tasks
16	The trust of my co-worker makes me feel that the information is secure at my workplace
17	There is no barrier between us at the workplace, and we exchange the information freely and securely
18	I do not feel that the visitors of nonemployees would impact the confidentiality and security of the information
19	I always put the information security among the priorities when dealing with others
20	I feel that the management exaggerates on the issue of information security in terms of the procedures and technology
21	Quality and efficiency of the used technology at computing center guarantee the security of the information and reduce my role in information security
22	Among the obstacles of the information security is the absence of a law to punish the cyber-criminals
23	The weakness of the awareness of the misuse of technology, e.g., sabotage and intrusion, is an obstacle to the information security
24	The availability of many free internet tools (spying, spoofing, hacking, etc.) make the sabotage/vandalism available for novice users
25	Hackers/attackers cannot be prosecuted because they are from other countries

Table AI. Employees questionnaire's statements

Appendix 2

No.	Statement
1	We have policy and procedures that control the daily business to assure information security
2	We have/plan to have international certification (e.g., ISO27001/BS-7799) to assure the quality of information security process
3	When designing and building the software systems, information security is considered as one of the major issues of system design and development
4	The information security procedures are written and available to all employees to follow
5	We have an information security technical plan (quarterly, half yearly, yearly) that we implement and follow
6	Information security procedures are clear and understandable for all employees
7	All employees are required to consent for the information security policy and procedures
8	Employees are not permitted to bring storage devices (USB flash, CD, DVD, etc.) into the computing center
9	Employees are not permitted to move storage devices out of the computing center
10	Non-authorized employees are strictly not permitted to enter the computing center
11	Information security experts are available at the computing center
12	We have an emergency plan and clear procedures to follow in case of any emergency or threats to occur
13	The computer machines are frequently examined to recycle the outdated ones in a way that assures the security of the confidential information
14	We have technical procedures to follow by the employees to update their computer machines for any security vulnerability
15	We have an information classification scheme to distinguish the confidential information from the public ones
16	We apply precise procedures for the employees' recruitment to work with confidential/sensitive information
17	We assure that the employees understand their duties before appointing them to prevent any misuse of the computing center's resources and/or possible deliberate act of theft
18	We have procedures for contractors' access to the computing center to assure the information security
19	We monitor the employees' commitment to the policy that obligates them to update their computer machines against any security vulnerability
20	We have certified/trained employees on information security (e.g. CISSP, SSCP, ICSA, Security+)
21	We train our employees at the computing center to improve their skills to perform their daily business securely
22	We schedule the operating systems' updates for the servers and employees desktops on regular basis to block any security vulnerability
23	We scan the storage devices, such as CD, DVD, USB, for any viruses before being used at the computing center
24	We update the anti-virus and anti-spam software on regular basis
25	We use access control tools to access sensitive locations and computer machines (e.g. fingertip, password, magnetic card, etc.)
26	We use hardware protection systems (anti-fire, backup protection, etc.)
27	We use cooling, heating, and ventilation systems to assure the safety of the data storage devices
28	Employees are not permitted to install any software into their desktop computers without the permission of the system administrator
29	We have backup systems for electrical power and communication in case of electrical/communication failure
30	We have data backup procedure that is performed on daily/weekly/monthly/yearly basis
31	We have protection systems such as hardware/software firewall, IDS systems, etc.
32	We have cryptography systems (e.g., encryption-based solutions)

(*continued*)

Table AII. Managers questionnaire's statements

No.	Statement
33	We apply content filters on incoming web requests
34	We have scanning and analysis tools to detect spying programs
35	We educate our employees on regular basis, on the importance of the information security and the impact of their daily business on the protection of resources at computing center
36	Among the obstacles of the information security is the absence of a law to punish the cyber-criminals
37	The weakness of the awareness of the misuse of technology, e.g. sabotage and intrusion, is an obstacle to the information security
38	The availability of many free internet tools (spying, spoofing, hacking, etc.) make the sabotage/vandalism available for novice users
39	Hackers/attackers cannot be trailed/punished because they are from other countries

Table AII.

About the author

Zakarya A. Alzamil holds a PhD in computer science from the Illinois Institute of Technology, Chicago, USA. His research interests are software testing, software engineering education, information security and quality assurance. He is an IEEE Senior member, and currently is an Associate Professor at the Software Engineering Department, King Saud University, Saudi Arabia. Zakarya A. Alzamil can be contacted at: zakarya@ksu.edu.sa