Al-Izki, Fathiya and Weir, George R S (2016) Management attitudes toward information security in Omani public sector organisations. In: 2016 Cybersecurity and Cyberforensics Conference (CCC). Institute of Electrical and Electronics Engineers Inc., Piscataway, NJ, pp. 107-112. ISBN 9781509026579 , http://dx.doi.org/10.1109/CCC.2016.28

Management Attitudes Toward Information Security in Omani Public Sector Organisations

Fathiya Al-Izki & George R. S. Weir
Department of Computer and Information Sciences
University of Strathclyde
Glasgow, UK
fathiya.alizki@strath.ac.uk, george.weir@strath.ac.uk

Abstract— The incorporation of ICT in public sector organisations is progressing rapidly in Oman where the government sees this as a means to enhance the delivery of online services. In this context, preserving the security of information, and making Information Security a core organisational aspect in public sector organisations, requires attention from management. Our research is the first known attempt to gauge management attitudes toward Information Security in Oman. We also consider how such attitudes influence Information Security governance. In addressing these issues, we review current compliance with Information Security procedures in Omani public sector organisations; review management attitudes toward Information Security governance practices; and explore how management attitudes toward Information Security impact upon these aspects.

Keywords— Information Security, Organisational Culture, Management Attitude, Information Security Policy, Information Security Training and Awareness

I. INTRODUCTION

Information Security (IS) in organisations aims to protect information assets, in part, by influencing employees' security behaviour [1]. This is increasingly important in organisations because the role of digital information becomes more important over time [2]. Additionally, IS effectiveness is highly correlated with the commitment of management towards its procedural and technological aspects. This commitment is the cornerstone to IS growth and maintenance as well as its related processes and culture. Accordingly, 'tone at the top, in other words, the security attitude espoused by influential senior people, is considered by virtually all assurance and security practitioners to be highly relevant to the success of security–related activities' [3].

II. PROBLEM STATEMENT

Information Security, a subset of overall security in organisations, depends mainly on organisational culture and, in particular, the development of an internal Information Security culture [4]. This study explores how 'Information Security culture' in the public sector is derived from management attitude and is, in turn, considered as a predictor of Information Security posture. Public sector organisations in Oman were examined as a case study for this research.

III. STUDY SIGNIFICANCE:

This study is the first in Oman that aims to gauge management attitudes towards Information Security, as well as the relationship between this attitude and associated governance issues. Attention is focussed upon 'tone at the top' or the management style. Additionally, this research characterises Information Security posture in Omani public sector organisations and adds a new scientific study to the area of Information Security in Arab countries, and Oman in particular, that will, hopefully, bring more attention to Information Security and positively influence the way it is considered in public sector organisations.

IV. STUDY QUESTIONS:

A primary aim is to characterise the management attitude towards information security in Omani public sector organisations. To this end, we address a series of related questions:

1- What is the compliance level of procedural information security in Omani public sector organisations?
2- What is the level of management good governance practices with regard to Information?
3- What is the relationship between management attitude towards Information Security and associated management governance activities?
4- What is the relationship between management attitude towards Information Security and compliance with Information Security policies?

V. LITERATURE REVIEW:

There is little doubt that management has an obligatory role toward Information Security. In our literature review management attitude towards Information Security was viewed from two perspectives, which are considered complementary to each other:

1. Management governance of Information Security by shaping the organisational culture.
2. Management's own commitment to good governance of Information Security, regardless of any organisational cultural context.

One aim of this study is to highlight that the organisational cultural context is not the only way to approach management behaviour with regard to Information Security. Committed managers promote and maintain good governance of Information Security whether or not their efforts are based on cultural factors. While many managers acknowledge the

significance of culture, most do not appreciate the roles and responsibilities they have in its development [5].

While management need not focus on organisational security culture as an explicit perception, the attitude they display to their subordinates, through involvement in daily operations regarding Information Security, will influence employee's compliance with security rules and practices. Management have the authority to influence other employees and are more likely to succeed in overcoming organisational resistance and cultural barriers [6]. When employees believe that management cares about security, they become more inclined to cooperate to improve security [7].

A. Governance of IS by shaping organisational culture

The role of management is important in the development of organisational culture and cultural change. Management is able to ensure sufficient allocation of resources and act as a change agent to create a favourable environment [8]. Indeed, an argument can be made that the concepts of Information Security culture and organisational culture may be interrelated [9]. Creating a safety culture within the organisation may encourage employees to take an interest in information security and help to shape effective information security within the organisation [10]. There is a need for leaders to realize that information is a strategic resource and to be informed, motivated, and engaged with regard to Information Security [11]. It is for them to take into account, not only the technological aspects, but also the behavioural and procedural aspects with Information Security [12].

B. Management commitment to good governance of IS

According to Zohar [13], the commitment of management is a prerequisite to any improvement in safety. Such commitment increases levels of motivation and safety concerns throughout the organisation [14]. Furthermore, a committed management provides the means and support for the development and implementation of safety. This is ultimately reflected by efforts to ensure that every aspect of work and each task component in the organisation (equipment, procedures, training, and planning) is regularly evaluated and, if necessary, modified toward potentially improving security [15].

The involvement of top management is crucial in the establishment, maintenance and success of actions relating to Information Security [16]. Their support is essential in obtaining involvement of workers to Information Security [16]. Of course, there are many factors that influence leaders' involvement in Information Security management. Significant differences in terms of age, education level, and experience in a given function are indicated [17].

C. Middle management

Many authors illustrate the middle manager's fundamental role in the development and implementation of strategies and organisational change. Payaud, argues that these managers continue to occupy a privileged position in organisations, at the interface between the action and policy decisions, claiming that they are more than the transmission belts; they can be change agents, knowledge transfer facilitators, innovators, key strategic players and coaches to their employees [18]. Thompson et al. differentiate the influence of high-level executives from that of middle management. They found that executives' guidance influences safety behaviour by communicating what is brought to their attention, while middle managers do so by their benevolent interactions with employees [19].

Further studies suggest that cooperation between employees and managers would be the highest influencing factor on most employees' safety behaviours [20], with such support and involvement of managers sending powerful signals throughout the organisation [21].

VI. METHODOLOGY, TOOLS AND SAMPLE

Our approach in this study comprised two initiatives. Firstly, we undertook a survey of relevant literature, to shed light on the management role in shaping good IS governance. Secondly, we deployed a survey questionnaire to assess the Information Security posture within Omani public sector organisations, as well as the Omani managers' attitude towards Information Security. Survey questions targeted (4) dimensions:

1. Organisation's Information Security Policy
2. Organisation's compliance with IS best practices
3. Information Scurity Training and Awarness
4. Managerial attitude towards Information Security

These four dimensions were specified as (32) aspects of Information Security. The survey, was conducted anonymously and was disseminated electronically via the Internet to all participants. Questions were written in Arabic and English to accommodate the native language and working language of participants.

The questionnaire consisted of (3) sections: demographic information, Information Security aspects and finally the respondent's notes and suggestions, with items rated on a Likert scale of (3) points (Yes, No, Not sure).

Following Sampieri, 'the instrument of data collection really represents the variables we have in mind. If it doesn't, our measure is deficient and therefore the study is not worthy to be taken into account' [22, p.285]. Data was analysed manually and using the software tool SPSS (v22), to characterise the posture of Information Security and to measure the strength and direction of association between the Information Security posture and managers' attitude towards Information Security.

Sample

The target population for this study was all employees working in the Omani public sector. Selection of individuals who are part of the sample is essential to determine that the obtained conclusions can be extrapolated to the total population. Therefore, the sample should be representative of the total population. In this study, a simple random sample was selected, to make reliable estimates for the population as a whole.

VII. DATA ANALYSIS

This section presents the analysis of the data collected by the survey questionnaire that forms the basis for the study. In the analysis, percentage was used instead of frequency to represent the perspective of the population sample towards the queried IS-related elements. This is considered a good way to show relationships and comparisons, either between categories of respondents or between categories of responses [23],

especially as there were many respondents who did not respond to some questions or marked some questions as "NA", (i.e. not all respondents answered all questions). Therefore, only the number of persons who actually answered any particular question is used in calculating the percentage.

Additionally, averaged percentage was used to indicate the overall posture of Information Security aspects. The average percentage would be calculated, for every scale item in any dimension, by dividing the total number of responses of every scale item in the dimension by the total number of responses to all questions of that dimension.

A. Information security status in Omani public sector

The status of Information Security in the Omani public sector was explored by investigating the level of compliance with IS best practices.

B. Organisations' Information Security policy

Answers from the survey respondents with regard to Omani public sector organisation's Information Security Policy are indicated in Table 1. A high percentage of "Yes" answers (above 50%) indicate a good status with regard to Information Security policy related best practices. This also indicates that the respondent is very likely to be working in an organisation concerned about information security. The measurement scale, reflecting the 5 questions, indicates the extent to which such organisations are concerned about Information Security policy and the degree of compliance with its related practices.

Table 1 shows that the respondents who marked "Yes" were less than 50% to all questions related to Information Security policy except for the question "Does the Organisation have a strong and enforced Information Security policy?", which was marked "Yes" by 65% of respondents. The average percentage of participant's positive perception toward Information Security policy is 33%.

C. Organisations' Procedural IS best practices

Table 2 shows answers from the survey respondents regarding the application of Information Security policy best practice in Omani public sector organisations. The measurement scale contains 13 questions. A high percentage of "Yes" answers (higher than 50%) indicates strong compliance with such practices.

It is clear from Table 2 that many Information Security practices have moderate levels of compliance: security background investigation for new employees (59%), the organisation using access control to manage the separation of duties (54%), removing all access rights and network accounts at employment termination (51%), prohibiting suppliers from accessing the organisation's network (50%). Some practices are on the low compliance side. Specifically: having a physical separation between the organisation's network and the Internet (41%), prohibiting short contract employees from accessing the organisation's network (19%), and restricting the use of mobile phones within the organisation premises (13%). The average percentage of compliance with Information Security best practices, from the perspective of the respondents is 40%.

D. Organisations' IS Training and Awareness

The measurement scale contains 5 questions that expose respondents' perspectives on the level of Omani public sector organisations compliance with the best practices regarding Information Security training and awareness. The results shown in Table 3 show that respondents who marked "Yes" were less than 50% in all questions. The average percentage of participants' positive perception toward Information Security training and awareness is 33%.

E. Organisations' Managerial Attitude towards IS

Management attitude was assessed via 10 items selected on the basis of the framework derived from the past literature and cultural views [9]. The measurement scale contains 10 questions. Table 4 shows respondents' answers to those questions, which reflect their perspective with regard to the management attitude towards Information Security in Omani public sector organisations. This table shows that all questions have been answered positively by less than 50% of the respondents. The average percentage of participant's positive perception with regard to managers' attitude towards Information Security in Omani public sector organisations is 24% and suggests that such attitude is not supportive.

F. Relationship between management attitude and Information Security in Omani public sector organisations

The relationship between management attitude towards Information Security and management IS governance activities is represented by two aspects: Information Security policy and Information Security training and awareness. The relationship between such an attitude and employee compliance with Information Security policies in Omani organisations was also investigated. These associations were assessed through the correlation between dependent and independent variables, defined as follows:

Dependent Variables: (i) Information Security policy, (ii) Information Security training and awareness and (iii) compliance with Information Security policies.

Independent Variables: management attitude.

To make responses to queried items more manageable, the concept of composite variable was used. The dependent variables are composite; which means that each is determined by combining the responses to a group of questions that, together, reflect the associated Information Security aspect. Additionally, the independent variable, which denotes management attitude to Information Security, is also a composite variable that combines responses to the questions that reflect such an attitude.

Hypotheses

To test the effect of management attitude towards Information Security and associated management governance activities, the following hypotheses were formulated:

H1: There is a positive relationship between organisation culture and the management governance activities regarding Information Security policy in Omani public sector organisations.

H2: There is a positive relationship between the management attitude regarding Information Security and management governance activities regarding Information Security training and awareness in Omani public sector organisations.

H3: There is a positive relationship between the management attitude regarding Information Security and compliance with Information Security policies in Omani public sector organisations.

Analysis

A Spearman's rank-order correlation was used to evaluate the relationship between management attitude towards Information Security, represented by the composite variable OrgISMA and the 3 composite variables: organisation's attitudes to Information Security Policy (OrgISP), Information Security Training & Awareness (OrgISTA), and Information Security Policy Compliance (OrgISPC). The results (detailed in Table 5) indicate the following.

(i) There is a strong, positive correlation between OrgISMA and OrgISP, which is statistically significant (rs = .715, p = .000).

(ii) There is a strong, positive correlation between OrgISMA and OrgISTA, which is statistically significant (rs = .814, p = .000).

(iii) There is a strong, positive correlation between OrgISMA and OrgISPC, which is statistically significant (rs = .851, p = .000).

Accordingly, the null hypothesis for the 3 hypothesis H1, H2 and H3 was accepted.

VIII. CONCLUSION

This study aimed at shedding light on Information Security as a management issue. In particular, the literature highlights the importance of management in Information Security, through shaping the organisational culture and through commitment to good governance.

Analysis of the survey responses indicate the perceived level of management good governance practices with regard to Information Security and how this could affect the compliance with procedural Information Security in Omani public sector organisations. Our results are:

1. *The average percentage of participant's positive perception with regard to such interest is 24%.*
2. *The posture of Information Security policies is below average 40%.*
3. *The compliance to Information Security policy best practices is 33%.*
4. *The average percentage of participants' positive perception towards Information Security training and awareness is 33%.*

These four points signify a considerable lack of management interest in Information Security in Omani public sector organisations and that the Information Security posture in Omani public sector organisations is not optimal. Additionally, analysis of the survey results also showed:

5. *There is a strong relationship between management attitude towards Information Security and aspects denoting the management governance activities (i.e., Information Security policy and Information Security training and awareness).*
6. *There is a strong relationship between management attitude towards Information Security and compliance with Information Security policies.*

We conclude that management attitude is a driver of Information Security governance in Omani public sector organisations and agree that management commitment can increase Information Security compliance in public organisations [24].

References

[1] AlHogail, A. & Mirza, A. Information security culture: A definition and a literature review, Computer Applications and Information Systems (WCCAIS), 2014 World Congress,17- 19 Jan. 2014

[2] Barlette Y. (2012), Vers une implication et une action des dirigeants de PME dans la sécurité de leur système d'information, Presses des Mines.

[3] Krag Brotby, W. & Hinson, G. (2013), PRAGMATIC Security Metrics: Applying Metametrics to Information Security, CRC.

[4] Richards, D.A., Oliphant, A.S. & Le Grand, C.H. (2005), GTAG1: Information Technology Controls, The Institute of Internal Auditors.

[5] Kane Urrabazo, C . (2006), Management's role in shaping organisational culture. Journal of Nursing Management 14, 188–194.

[6] McCrohan K. & Dutta A., (2002), Management's role in information security in cyber economy, California Management Review, (45) 1, 67-87.

[7] Choudhry, R. M., Fang, D., & Mohamed, S. (2007), The nature of safety culture: A survey of the stateof-the-art. Safety Science, 45(10), 993–1012.

[8] Kankanhalli A., T. Hock Hai-CYT and Bernard Kwok-Kee W., (2003), "An integrative study of information systems security effectiveness", International Journal of Information Management, (23), 139-154.

[9] Lim, J.S., Chang, S., Maynard, S. & Ahmad, A. (2009), Exploring the Relationship between Organisational Culture and Information Security Culture, 7th Australian Information Security Management Conference.

[10] Van Niekerk, J.F., and Von Solms, R. 2010. "Information Security Culture: A Management Perspective," Computers & Security (29:4), pp 476-486.

[11] Rockart, J.F. & Crescenzi AD., (1984), "Engaging top management in information technology", Sloan Management Review, (25) 4, 3-16.

[12] Boss, S.R., Kirsh, L.J., Angermeier, I., Shingler, R.A. & Boss, RW (2009), "If someone is watching, I'll do what I'm Asked: mandatoriness, control and information security", European Journal of Information Systems, (18) 151-164.

[13] Zohar, D. (1980). Safety climate in industrial organisations: theoretical and applied implications. Journal of Applied Psychology, 65(1), 96

[14] Lee, T. (1998). Assessment of safety culture at a nuclear reprocessing plant. Work et Stress, 12(3), 217–237.

[15] Wiegmann, D., Zhang, H., von Thaden, T., Sharma, G., & Mitchell, A. (2002). A synthesis of safety culture and safety climate research. University of Illinois at Urbana-Champaign, Aviation Human Factors Division

[16] Johnston, A.C. & Hale, R. (2009), "Improved Security through Information Security Governance", Communications of the ACM, (52) 1, 126-129.

[17] Song, J.H. (1982), "Diversification strategies and the experience of top executives of wide firms", Strategic Management Journal, (3), 377-380

[18] Payaud, M.A. (2005). Formation des stratégies et middle managers. Paris : L'Harmattan.

[19] Thompson, R. C., Hilton, T. F., & Witt, L. A. (1998). Where the Safety Rubber Meets the Shop Floor: A Confirmatory Model of Management Influence on Workplace Safety. J. of Safety Research, 29(1), 15–24.

[20] Simard, M. & Marchand, A. (1997). Workgroups' propensity to comply with safety rules: the influence of micro-macro Organisational factors. Ergonomics, 40(2), 172–188.

[21] Grover V. (1993), "Empirically derived model for the adoption of customer-based inter-organisational systems", Decision Sciences, (24) 3, 603-639.

[22] Sampieri, R. (1991). Research Methodology, Mexico: McGraw–Hill.

[23] Taylor-Powell, E. (1989), Analyzing quantitative data, http://learningstore.uwex.edu/assets/pdfs/g3658-6.pdf

[24] AlKalbani, A., Deng, H. and Kam, B. (2015), Organisational security culture and information security compliance for e-government development: the moderating effect of social pressure, 2015.
.

Table 1: IS Policy

Questions on IS policy	% age	No. of "yes" answers	Total no. of answers
1. Does the Organization have a strong and enforced Information Security policy?	65%	57	88
2. Are employees educated about any updates in the Security policy?	30%	26	87
3. Is a hard copy of "IS" policy is signed by all?	29%	24	82
4. Is the IS policy reviewed and updated periodically ?	25%	22	87
5. Does the Organization monitor IS policy violation periodically?	17%	15	87
Average percentage	33%	144	431

Table 2: IS Best Practices

Questions on IS best practices	Public	No. of "yes" answers	Total no. of answers
1. Is the security background investigated when recruiting new employees?	59%	41	70
2. Does the Organization use access control to manage the separation of duties?	54%	38	70
3. Are all access rights and network' accounts removed at employment termination?	51%	36	70
4. Are suppliers prohibited from accessing the Organization's network?	%50	35	70
5. Are there certain security measures followed by the Organization to secure classified documents?	49%	34	70
6. Are network firewall logs and server logs monitored regularly for intrusion attempts?	48%	24	50
7. Are there certain procedures to secure laptops usage in meetings and businesses?	45%	31	69
8. Is there a physical separation between the Organization's network and the Internet network?	41%	29	70
9. Is there a disciplinary process applied when an IS violation is repeated?	39%	23	59
10. Is there a ready Disaster Recovery Plan in the Organization?	32%	22	68
11. Is copying documents and data into external storage devices restricted?	%21	15	70
12. Are short contract employees prohibited from accessing the organization's network?	%19	13	70
13. Is the use of mobile phones restricted within the organization premises?	%13	9	70
Average percentage	40%	350	876

Table 3: Management Attitude to IS

Organizations' Management attitude towards Information Security (IS)	%Age	No. of "yes" answers	Total no. of answers
1. Do managers at all levels support IS policies?	38%	30	78
2. Are employees enforced to commit to the IS policy?	32%	20	63
3. Does the organization's IS get an adequate management interest?	31%	21	67
4. Is there an assigned annual budget to develop IS?	29%	23	78
5. Is the organization interested in consulting internal or external IS auditors to insure that full security is provided to its projects and systems?	26%	17	65
6. Are security officers exercising their role to the fullest?	26%	19	73
7. Does the organization motivate employees when notifying superiors in the event of an IS violation?	19%	13	70
8. Do you think Managers care of IS at all times (not only when there is a breach of Security in the organization)?	18%	14	78
9. Is practicing good IS is part of the shared beliefs of organization members?	9%	4	45
10. Are IS policies applied to all organization members including managers in different levels?	4%	2	53
Average percentage	24%	163	670

Table 4:

Information Security training and awareness	%age	No. of "yes" answers	Total no. of answers
1. Is there a regular knowledge update for the IS staff?	44%	34	77
2. Does the organization conduct adequate training programs on IS for all employees?	37%	29	79
3. Does the organization conduct refreshing programs on IS for employees	30%	24	79
4. Are hard copies of the IS policy distributed so that all employees are aware of it?	21%	18	87
Average percentage	33%	105	322

Table 5: Composite Variables

Spearman's rho		OrgISMA
OrgISP	Correlation Coefficient	.715
	Sig. (2-tailed)	.000
	N	116
OrgISTA	Pearson Correlation	.814
	Sig. (2-tailed)	.000
	N	116
OrgISPC	Pearson Correlation	.851
	Sig. (2-tailed)	.000
	N	116