Proc. of the Intl. Conf. on Advances in Social Science, Management and Human Behaviour-- SMHB 2013

ISBN: 978-981-07-7965-8

Heuristics to evaluate Organisational Information Security Culture

Ibrahim Al-Mayahi, Sa'ad Mansoor

***Abstract*— Information Security Systems are a set of systems, policies and procedures put in place to protect information and ensure access to information is only available to sanctioned users of the system. Whilst hardware and software components are always essential in the safe-guarding access to digital information, in evaluating the security of an information system is it essential to consider the behaviour of human users who form an integral component of the system. The Information Security Culture of an organisation reflects the set of behaviours of human operators where these behaviours may impact on the security of organisations information. This paper demonstrates the evaluation of particular e-Government organisations Information Security through questionnaire.**

***Keywords*— e-Government, Information Security Management, Orgnisation Security Culture**

I. Introduction

Controlling the spread of information has been essential to the provision of all kinds of human security since the dawn of civilisation. The dissemination of information is essential for organisations of any scale to function effectively, yet at the boundaries there has always been the need to prevent the dissemination of some information to safe guard an organisation from its malicious use. Creating systems that allow efficient communication of secure information within an organisation yet preventing it leakage to the outside is a central challenge to Organisation Management.

As information technology has progressed from paper based to digital systems the amount of information being managed by organisations, and the need to secure it, continues to rise exponentially. Despite the huge amount of work that has been done to create secure hardware and software systems, the behaviour of human users, effectively the user's culture, is much less readily changed. Any Information Security System layer is only as strong as its weakest component and very often the behaviour of human operators are the weakest part. When an individual's behaviour does not adhere to security policies then weaknesses in security are made. Whilst a strong set of policies and practices is therefore essential to the Information Security of an organisation, they are not in themselves sufficient and it is only when these practices have be adopted and permeated deeply in to the organisations Information Security Culture that organisations information may be considered secure.

Ibrahim Al-Mayahi,
Ministry of Interior
United Arab Emirates

Dr Sa'ad Mansoor
School of Computer Science
Bangor University
UK

Government is the administration of a society, and to be effective needs to have information which malicious members of society cannot utilise to the detriment of society. To be more effective Governments have adopted digital information systems create e-Government systems to deliver administrative services to society via digital network.

E-Government enables digital interaction and information transfer between citizens, business, and public sector organisations. The majority of national governments have introduced some form of e-Government program ranging from a minimal informational web system to advanced implementations providing a suite of interactive services of ever increasing sophistication and scope. Improving the efficiency, accessibility and effectiveness of public service delivery is a driving challenge of E-Government strategy the world over [1].

Within the e-Government human users administer digital information systems; and their behaviour is a key factor determining the information security within the e-Government. Collectively we term all behaviours of these users with regard to information security the Information Security Culture of the organisation.

Organisations cannot achieve effective information security without the establishment, implementation, and maintenance of a clear and rigorous information security policy [2]. The formulation and utilisation of information the security policy can enhance the effectiveness of ISM system [3]. Simply establishing a policy is of course not in itself sufficient as it does not guarantee that individuals will comply with the policy. As a result, policy enforcement is essential. In addition, there is a need for organizations to ensure their information security policy is structured and organized effectively [4].

There is a danger that Information Security Policies may be resisted where they appear to be in conflict with social expectations of politeness or trust, in these cases an Information Security Culture has yet to be fully adopted and is in conflict with traditional social culture. Social engineers will exploit these situations to maximum effect, leveraging the full weight on cultural expectation in order to shame, humiliate or extract sympathy from an organisation worker, so as to persuade them to depart from the correct Information Security Policy [5].

Proc. of the Intl. Conf. on Advances in Social Science, Management and Human Behaviour-- SMHB 2013

ISBN: 978-981-07-7965-8

II. Evaluating Information Security Culture

In order to evaluate an organisation Information Security Culture, 6 different areas in the behaviour of the organisations workers were investigated. For each of these a sample of the organisations workers completed a questionnaire, where answers on a likert scale graded 1-5. We take 3 to be the minimum satisfactory score for each question and a mean result below 3 from the sample indicating an area of concern. For each area we are able to produce an average mean across all questions providing a heuristic of the security of the organisations culture in this area. We describe each area and the associated questions below.

A. *Policy*

The first step of establishing a robust government security environment is to define the Policy, which is an essential part of security practices within organisation and can substantially influence organisational security. As Higgins [6] notes, "Without a policy, security practices will be developed without clear demarcation of objectives and responsibilities". The organisation will face major difficulties when implementing ISM System. The primary objective of the information security policy is to define the users' rights and responsibilities regarding information within an organisation [2]. Effective information security policies will help users understand what is acceptable and responsible behaviour regarding information resources and will assist in establishing a safe information environment [7].

Policy is on the top of the management structure and plays the role of setting up the guiding principles for the rest of the organisation. Policy is also an essential part of leading people in an organization. Clear policy defines roles and responsibilities of the team. Hence policy can also help in the efficiency of the operations of information security protections. Below is a list of questions used to address the organisation policy.

[1] The Organization's Security Policy is comprehensive and complete.

[2] There are formal and specific procedures to report security violations.

[3] The organisation has put on place rules on how to report information security violations.

[4] I know the person in charge of reporting cases of abuse or damage relating to electronic resources of the Organisation.

B. *Strategy*

After defining the Policy, the Security Strategy should be selected to indicate the approach for government to reach their information security protection goals. There are many different ways to complete the tasks of security protection, an overall Security Strategy with many sub-strategies enables the organization complete the security protection tasks effectively, efficiently, economically and then meet the strategic goals of information security.

To define a Strategy, an overall goal and strategic goals should be raised first by the management. The Security Strategy should align with the Policy toward the goals of government security management. The questions used to evaluate this section are listed below.

[1] .I know there exists of Information Security Policy in my Organization There are formal and specific procedures to report security violations.

[2] Information security policy covers the goals and objectives of the organization.

[3] Information Security Policy covers all the information security previsions required within my department.

[4] The Security Policy Goals are sufficient and clear.

C. *Knowledge*

Knowledge is a corner stone of the successful administration of information systems. Understanding the technical nature of some Information Security issues require in depth knowledge of the relevant technology in order to understand how weaknesses can occur. In addition users need to understand the deployed security technology, as well as be able to make risk assessments, risk treatments and implement the relevant information protection techniques.

For e-Governments the knowledge of security management must acquire and maintained and transferred to the security management teams. The knowledge may be acquired from the external resources or researched and developed by the Security Team. 3rd parties, vendors of security solutions and the national security agencies may all provide Knowledge. A knowledge management mechanism, database or tools should be implemented for better security management. The questions used to evaluate this section are listed below.

[1] Information Security is Information Confidentiality.

[2] Information security is the integrity of information.

[3] Information security is the Availability of information as requested by the authorized person

[4] Employee training on the optimal use of his own tasks, especially in terms of security, reduces lots of risks and gaps, and eliminate professional and security related faults.

[5] The training courses attended were enough to make use/provide the e-services in secure.

D. *Confidentiality*

Confidentiality of government information is the first priority of security management. Confidentiality is important to the security management of government because most government information need to be protected to protect the rights of civilians or the operations of government. In order to keep a secure environment, Confidentiality should be defined and implemented by establishing policy, regulation and

Proc. of the Intl. Conf. on Advances in Social Science, Management and Human Behaviour-- SMHB 2013

ISBN: 978-981-07-7965-8

procedures. Confidentiality regulates the government users to keep the information secure and should be base on, and supported by, the overall Policy. The questions used to evaluate this section are listed below.

[1] We have clear policies on how password in term of length and use must be handled.

[2] Use of weak password or indifference to the protection of the password may endanger the safety and confidentiality of the contents and systems.

[3] In case of subcontracting with a 3rd party company in charge of e-government systems and devices maintenance, the safest way is to create a temporary account for them, and then delete it when contract finishes.

E. *Compliance*

Compliance helps an organization to meet its internal and external requirements. For information security, the compliance process pushes the staff to follow the internal security management requirement and on the other hand, guiding the organization to meet the legislation and regulation requirements. In a P-D-C-A cycle (the Deming Cycle of management), Information Security Policy is established in the Plan stage and aims to be the top tier of guidance for the whole management system. Information Security Compliance utilizes compliance checking in form of audits or reviews and checking to assure the planned policy and procedure of management system are all executed effectively, as well as the requirements that come from partners or governments. These two tools of management should be integrated and operated seamlessly to ensure an effective information security management.

Compliance processes help organizations compare their actual information security operations with international ISM standards. Compliance evaluates and audits the difference between the expected standards of organizational situations, and the reality in the organization. Evaluating the degree of compliance helps organizations determine their conformity to the controls listed in the standards, and delivers useful outputs to the certification process for the next stage of ISM certification [8]. Compliance with internationally recognized standards is growing in importance, because it has become popular as a common basis for information security measurement. The questions used to evaluate this section are listed below.

[1] The management is committed to comply with Information Security Policy.

[2] My organization does enough to implement information security

[3] Staff are totally committed to achieve the Organization's Information Security goals

[4] I adhere literally to the policy in working to achieve the goals of the Organization Information Security Policy

[5] I know where to find the relevant information security policies, standards and guidelines

F. *Behaviour*

We term the employees' perceptions and attitudes, value and behaviour regarding information systems. Behaviour measures the collective values, norms and security awareness of users. In some case workers may develop an attitude of disregard for Security Policies if they perceive them as being unnecessarily draconian, or feel they do not grant room for common sense or rational judgement on the part of the worker, or where they present an excessive overhead on an employee's workload. It is only when workers are educated as to the Information Security threats that are the motivation for security policies that they make every effort to follow the prescribed protocols, which leads to the adoption of this new working culture [9]. The questions used to evaluate this section are listed below.

[1] I DO report to Security authorize personal for any security violation by colleagues /staff within my department.

[2] The security policies are strictly implemented without any exceptions.

[3] The computer and electronic communications systems should be used for UAE's business activities only use work equipment to perform. personal use, such as sending personal email or send SMS or access to news

[4] Under no circumstances, for example not even when I am away on vacation, am I allowed to pass my password on to someone else. If necessary, password can be given over the phone to information security officer to measure its strength

[5] In case of subcontracting with a 3rd party company in charge of e-government systems and devices maintenance, the safest way is to create a temporary account for them, and then delete it when contract finishes.

III. Results

To evaluate an organisation information security culture, the entire population needs to be included in the audit process. The population can be seen as all employees who are working in the organisation and have access to its information. This is necessary since the culture of one office to the next and one department to the next could be different. By getting all employees to participate, comparisons can be made between offices, departments and job levels. It is often unrealistic to involve all employees if the organisation has a large workforce, in which case a sample that is representative of the overall workforce demographic can then be used to participate in the audit. In this study four sectors of UAE e-Government were chosen, and 69 employees participated in the survey. This represents 30% of the work force within that department [5].

To ensure confidentiality, the questionnaires were answered

Proc. of the Intl. Conf. on Advances in Social Science, Management and Human Behaviour-- SMHB 2013

ISBN: 978-981-07-7965-8

anonymously, employees feel more confident giving honest and accurate opinions if they know they cannot be identified. The majority of the respondents were deputy mangers 43.3% and also technicians 31.9%, as shown in figure 1.

Table 1 shows the survey results using the mean and standard deviation, to measure the security culture within the organisation. It can be seen that the majority of the questions scored a mean greater than 3, and there is only one score below 2.5. This implies that the trend is toward the right side of the scale (good practices).

However, in this study it was recommended to set a target of a threshold mean score of 4, this is to make sure that the unsure answer is not acceptable. According to this assumption we can see that large number of answers doesn't meet the threshold and there are areas that required some improvement, as there mean is below the threshold

TABLE 1. TABLE TYPE STYLES

Factors	No.	Mean	St. Deviation
Policy	Q1	3.19	0.692
	Q2	3.36	0.950
	Q3	3	0.7588
	Q4	3.51	0.901
Strategy	Q1	3.72	0.873
	Q2	3.40	0.710
	Q3	3.42	0.695
	Q4	3.25	0.7799
Knowledge	Q1	4.4	0.875
	Q2	4.09	1.025
	Q3	4.00	1.007
	Q4	4.49	0.756
	Q5	2.93	1.146
Confidentiality	Q1	3.54	1.183
	Q2	4.47	0.775
	Q3	4.13	0.916
Compliance	Q1	3.50	0.812
	Q2	3.47	0.812
	Q3	3.23	0.904
	Q4	3.39	0.889
	Q5	4.23	0.618
Behaviour	Q1	3.12	0.856
	Q2	4.11	0.956
	Q3	2.71	1.33
	Q4	2.45	1.243
	Q5	3.06	1.475

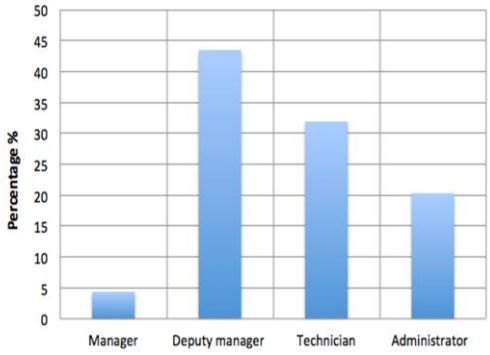

Figure 1. The profile of the survey corresponded

It is also evident that there is some questions score below 3 such as the behaviour section (Q2, Q3) and the knowledge section Q5. These areas require immediate attentions as it score below minimum acceptance level (mean = 3).

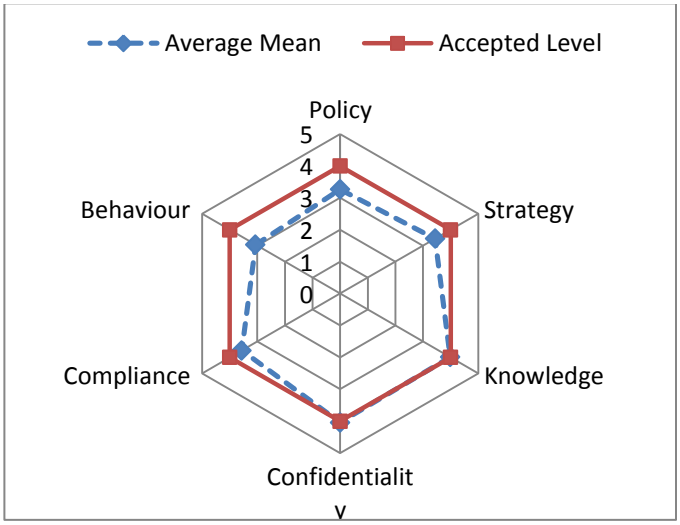

Figure 2. Information Security radar

To assess the information security perception of the employees by each area under study, the average mean for each area was plotted against the accepted threshold of 4. Figure 2 shown the results and it is obvious that the organisation employees respond to an acceptable level with regards to knowledge and confidentiality. While the other factors fell short. This implies that the employees need more training and education. There is also the need to change the staff behaviour toward the security risk within the organisation.

IV. Conclusions

All modern organisations have implemented a degree of culture of Information Security; however where this culture has not become pervasive and fully embedded in the organisation's culture, there remains a threat to the organisations Information Security. In order to identify potential weaknesses in the practices and behaviours of

ISBN: 978-981-07-7965-8

workers that may constitute such a threat, an assessment of an organisation Information Security Culture was carried out in form of questionnaire, this process lead to the continual Improvement of the organisations Information Security. Anonymous questionnaires are a key instrument for assessing the standards of Information Security in an organisation, being essential for evaluating the impact of any introduced measures such as training courses or new security policies.

The assessment has shown that generally the UAE e-Government has an adequate culture of Information Security. However, there remain some areas where management could facilitate further enhancement of the culture of information security by reviewing the organisation security policy based on these results. We recommend that training in security best methods be carried out within the organisation to ensure that all employees are aware of best practices within their departments. This should improve the employee's behaviour toward information security practices.

Acknowledgment

The authors would like to thanks the UAE Ministry of Interior for supporting this research.

References

[1] K. D. Mitnick, W. L. Simon, The Art of Deception: Controlling the Human Element of Security, John Wiley and Son, 1 edition, 2003

[2] Hong, K., Chi, Y., Chao, L., R., Tang, J. (2003). An integrated system theory of information security management Information Management & Computer Security, 11(5), 243-248.

[3] Fulford, H., Doherty N., F. (2003). The application of information security policies in large UKbased organizations: an exploratory investigation. Information Management & Computer Security, 11(3), 106-114.

[4] Von Solms, S. H., & von Solms, R. (2004). The 10 deadly sins of Information Security Management. Computer & Security, 23, 371-376.

[5] Ibrahim Al-Mayahi, and Sa'ad P. Mansoor, "Information Security Culture Assessment: Case Study". 2013 IEEE Third International Conference on Information Science and Technology (ICIST 2013). Yangzhou, China.

[6] Higgins, H. N. (1999). Corporate system security: towards an integrated management approach. Information Management & Computer Security, 7(5), 217-222.

[7] Höne, K., Eloff, J., H., P. (2002). Information security policy — what do international information security standards say?. Computers & Security, 21(5), 402-409.

[8] Karabacak, B., and Sogukpinar, I. (2006) A quantitative method for ISO 17799 gap analysis. Computers & Security, 25(2), 413-419.

[9] C.W. Axelord, Outscoring Information Security, Artech House.

About Author (s):

Ibrahim Humaid Al-Mayahi, is Engineer in the Ministry of Interior UAE, has BSc Electronic Engineering and MSc Information Security UK. His research interest is in the areas of data breaches, e-government information frameworks and information security systems.

Sa'ad Mansoor was appointed to the academic staff of the School of Computer Science in 2003. His research expertise lies mainly in the modelling of computer networks and information security. His research has been performed in close collaboration with academic and industrial research groups