An Analysis of Top Management Change on Information Security Management System

Dyana Zainudin, Humayun Bakht, and Atta Ur Rahman

Cardiff Metropolitan University, UK
Corresponding author's email: nuruldyanazainudin {at} gmail.com

ABSTRACT—*This paper analyse the concept to overcome the major impactfaces on Information Security Management System (ISMS) when the changes of top management in an organisation occurred. Change of top management in an organisation could reflect the whole processes as different leader have different ways in managing the organisation including goal, mission, vision, policies and plans. Many certified ISO27001 organisations have facing the problems during Internal Audit (IA) process when there are changes of top management in an organisation. This paper explores the possibility of concept in ensuring the change of top management doesn't affect the ISMS in place and contributes the key requirements for management activities in information security in order to make sure the information security process doesn't get affected when there are changes of top management.*

***Keywords*—**Information security, information security culture, quality management, change management.

1. INTRODUCTION

Level of management in each organisation is divided into three levels which are top management, middle management and lower management. This paper is emphasizing on top management role in committing with information security management. According to Zakaria et al, leading concept can be used as an influence to the employees to implement the daily information security process [3].

Influence in leadership can be varied by different tactics such as pressure, assertiveness, legitimating, coalition, exchange, upward appeals, ingratiating, rational persuasion, personal appeals, inspirational appeals and consultation[2].

However, the effectiveness of each tactics may cause different outcomes. It is believed that no matter what tactics is using by the leader, in terms of security, knowledge based in handling confidentiality, availability and integrity should be at least in intermediate level of every top management before influence the employee to implement the information security.

Based on ISO27001 requirements, besides oversee the whole process of ISMS, the top management main responsibility is to plan the information security policy, objectives, establish roles and responsibilities, provide resources, decide the risk assessment, ensuring IA are conducted and conduct management reviews.

Management reviews is the process to review results of IA, feedback from interested parties, techniques, products or procedures, decide on preventive and corrective actions, risk assessment, follow-up actions from previous management reviews and recommendations for improvement. All these process require knowledge in order to make decisions and the process is an ongoing each year process.

Decision of every management review is not only require thoughts but it requires costs such as improvise the information security monitoring system etc. If the top management does not have the knowledge in information security, they couldn't understand the important of information security continual improvement in an organisation. They could ignore or keep it pending for the next year management reviews.

In this point of view, the author emphasise that management commitment in implementing ISMS is the most important roles for the whole organisation. Therefore, knowledge of information security needs to be in a place for every top management members. If the knowledge of top management is part of ISO27001 requirements, the change of top management will not be affecting the whole organisation in implementing ISMS.

The further section will discuss the vulnerability of top management in influence the employees to implement the ISMS followed by the proposed solution in handling the change of top management in ISMS.

2. THE CONCEPT OF ISMS

In this section discuss the vulnerability of top management in influence the employees to implement the information security without having the knowledge of ISMS. The author will also discuss the common characteristics of information security culture and management activities in information security which created by Zakaria et al.

A. Top Management

The top management consists of Board of Director (BOD) and Chief Executive Officer (CEO) or some organisations called as Managing Director (MD) or President. It is believed that not many educational background among top management is from information security field as information security is one of specific area under information technology which empowered by information security expertise who certified with Certified Information Systems Security Professional (CISSP), Information Systems Security Management Professional (ISSMP), Information Systems Security Engineering Professional (ISSEP), Information Systems Security Architecture Professional (ISSAP), Systems Security Certified Practitioner (SSCP), ISO27001 lead auditor etc.

According to analysis by Yuan et al, most of the top management member is in higher diploma, at least associated degree in relevant to company's industry [4]. Which means, top management is not significantly have information security background in banking sectors or airlines industries etc. which the needs of information security implementation is very important for both sectors. Therefore, the influence in leading concepts in terms of security can't be fully developed without the knowledge of information security among top management. Further views about leading concept in information security will be discussed in section 3.0.

According to Zakaria et al, there is integration with 'leading' activities in management such as managing people, productions and operations in organisations in inspiring all staff to perform information security practices in organisations. However, to inspire all staff, the knowledge from top management is important to influence the staff to comply each of controls in ISMS. According to Kim DeKlein, leadership is a mix of knowledge, values, skills, and behaviours [1]. Without knowledge, the leader could not be fully delivered the messages to influence the staff.

B. Security Culture

According to Zakaria et al, in order to develop a security culture amongst employees in the organisation, the non-technical aspects should be taken cognisance which consider employees' security perceptions, design of basic security tasks, internalization of security knowledge, etc. This idea was suggested beside technical aspects as many who are involved in information security policies and procedures is understandably come from the technical background or information technology background [3].

He also stated that studies have shown that technical alone are not enough to handle internal security incidents. Therefore, in order to have better security precautions in organisations, both the technical and non-technical aspect of information security need to be addressed [3].

Zakaria et al has come out with common characteristics of information security culture based on the research findings which consist of i) shape employee behaviour towards security concerns ii) create a secure environment within an organisation and iii) require participation from all employees [3]. In the suggested characteristics, the author agreed that the culture should contain on shaping behaviour, create environment and the participation of employees in information security.

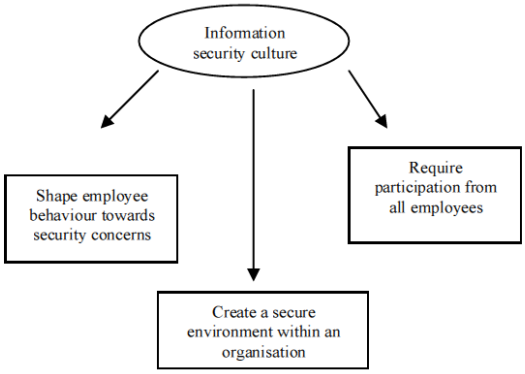

Figure 1: Common characteristics of information security culture [3].

Therefore, in the following section will discuss the top management role on developing those characteristics to be in place.

C. Top Management Role

Based on information security policy in international standard ISO27001:2005, the objective of the policy is to provide management direction and support for information security in accordance with business requirement and relevant laws and regulations. 'Management direction' can be explained as the policy created in an organisation must be involved a 'management commitment'.

The 'management commitment' could be elaborated byi) supporting the goals of information security in line with the business strategy and objectives, ii) setting controls for risk assessment and risk management, iii) compliance with legislative, regulatory, and contractual requirements, educations, training and awareness, business continuity management and consequences of information security policy violations, iv) incidents handling and v) documentation that supports policy such as procedures and security rules.

Those roles of top management in information security as stated in international standard are the first controls that shall be complied before proceed to the rest of the controls which consist of technical, administration, third parties and etc. Therefore, the question should be answered in the next proposed solution is 'how can the management develop the direction of organisations which involve information security if they have no background or knowledge about information security?' and if the current top management has knowledge and could direct the business well in line with information security, 'what if, the organisation has changed the rest of BODs or CEO/MD/President? Which do not have background in informations security', 'does the culture will change and the information security implementation is affected due to the changes?'

By referring to Hannagan concepts of planning, organizing, controlling and leading activities in order to accomplish organisational goal, Zakaria has proposed to reengineering the concepts by embedding information security to create security task to all employees, perform security tasks in daily work routines, guide employees to a proper security tasks and inspire everyone to perform security task.

The proposed reengineering concluded that management activities are important in order to develop appropriate information security culture. However, before each of the organisation to begin with the proposed reengineering, the question is 'how many of top management understand about information security in order to deliver the leading concept?'

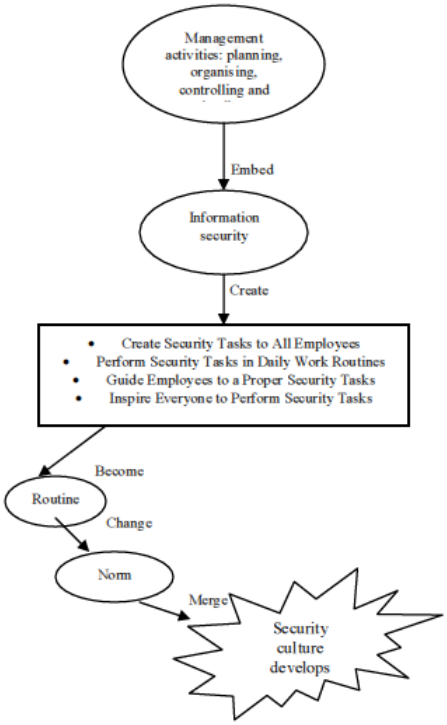

Figure 2: Embedding management activities in information security [3].

Next section will explain on the proposed solution in handling the change of top management affecting leading concept in ISMS.

3. PROPOSED SOLUTION

As discussed above, several questions have been highlighted in order to express concerns on the role of top management in managing information security in an organisation in ensuring that if the changes happened among top management, it couldn't effect the whole existed implementation of ISMS.

It is understandable that every organisation which have implemented information security in organisation or have certified with international standard ISO27001 have already assigned the expertise personnel to handle the controls and requirement that related to information security. However, that expertise can only deliver the three phases of information security which is do, implement and check. For plan phase, which is the first phase of information security based on

international standard, it will involve top management with the assistant of the assigned information security expertise. Top management is responsible to make a decision and oversee the whole phases of information security.

Therefore, the author would like to propose the solution of top management requirement in ensuring the changes of top management could not affecting leading concept in ISMS.

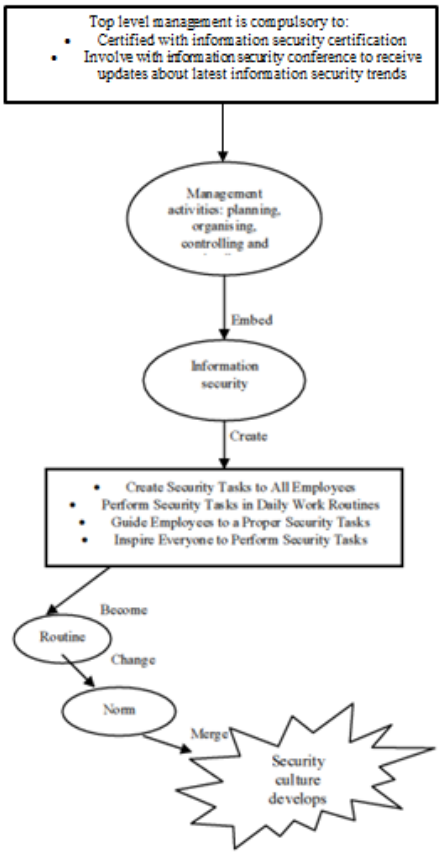

Figure 3: Top management requirements of ISMS

The two requirements needed for top management level to manage the organisation which implemented ISMS are i) to certified with information security certification and ii) to involve with information security conference to receive updates about latest information security trends.

A. Information Security Certification

There are many certification of information security according to role and responsibilities. Therefore, it is recommended for top management to have information security certification first before managing the whole ISMS in an organisation.

B. Information Security Conference

Information security conference is one of the platforms for the top management to know exactly the trends and latest update about information security. The discussion on information security could bring further knowledge and to continually improve the ISMS in an organisation.

It is believed that by granting the proposed requirements, it will strengthen the management activities in information security. As discussed above, influence in leadership only can be high affected if the knowledge can actually be in the mix of knowledge, values, skills, and behaviours. Without knowledge, the values, skills and behaviours are meaningless.

It is well known that BOD is the representative of shareholders and CEO/MD/Presidents is selected by the BOD. There is no one could question on their background etc. and it is beyond controls as long as they have share portion in organisation. However, as an organisation that seeks for certifications or awards, there are requirements that need to be fulfilled by the organisation in order to successfully qualify.

International standard for ISMS ISO27001 is globally used by the organisations. Those organisations which certified with ISO27001 needs to comply with all controls provided by the International Organisational of Standardisation in order to get certified. This certification gives benefit to the organisation such as market potential, customer trust etc. By having this certification, it is indirectly contributes to business profit.

Therefore, it is suggested that the requirement for having the certification is to make sure that the top management is certified with ISO27001 and include the involvement in information security conference as one of the top management's key indicator for ISO27001 certified organisation. By failing to do so, the certification will be suspended or not qualified.

4. CONCLUSION

Therefore, by having the two proposed requirements, the change of top management in an organisation could not affect the leading concept in information security if the proposed solution is applied to every top management in organisation that implement ISMS.

5. REFERENCES

[1] DeKlein, K., 1994. *Ontario.* [Online] Available at: http://www.omafra.gov.on.ca/english/rural/facts/94-081.htm [Accessed 2 May 2014].

[2] Hall, A., 2007. *NebGuide.* [Online] Available at: http://ianrpubs.unl.edu/epublic/pages/publicationD.jsp?publicationId=733 [Accessed 2 May 2014].

[3] Omar Zakaria, 2007. Reengineering Information Security Culture Formulation Through Management Perspective. p. 4.

[4] Yuan, L., 2011. Notice of Retraction Education background of Top Management Teams and the organisational performance of Small and Medium-sized Enterprises: Based on upper echolons theory. Issue IEEE, pp. 1-5.