A FRAMEWORK OF INFORMATION SECURITY CULTURE CHANGE

[1] AREEJ ALHOGAIL AND [2] DR. ABDULRAHMAN MIRZA
Department of Information Systems, College of Computing and Information Sciences,
King Saud University Riyadh, Saudi Arabia
E-mail: [1] alhogail@ccis.imamu.edu.sa , [2] amirza@ksu.edu.sa

ABSTRACT

Establishing information security culture within an organization may include transformation of how employees interact with the information assets which may be challenged with resistance, fear or confusion. Change management skills could assist organization members to smoothly adapt to the new culture. The use of change management in information security culture has been rarely investigated in the literature and very few models have been offered. This paper reviews the available change management models that have been used in information security management. Then it integrates a set of change management principles that were proposed in the literature and combine them to a comprehensive multistep framework that support and guide the transition in information security culture change within organizations. Moreover, the principles will be the base of suggestion of the appropriate guideline to support the effective implementation of change in information security culture. The framework provides guidance to information security professionals and academic researchers in taking proactive steps and measures to facilitate the culture change.

Keywords: *Change management, Information security culture, Culture change.*

1. INTRODUCTION

Achieving information security is a complex process that requires the investment in technology and in people as well. Procuring the advanced security technologies does not necessarily lead to secure environment as their performance critically depends on how they are implemented. It requires developing the necessary employees' skills and engaging them in the process. Many researchers suggest that establishing information security culture would reduce internal threats to information security and will enable staff to be more aware of the risks and of their responsibilities, thereby acting in a sensible and secure manner [1].

Alhogail & Mirza [2] defined information security culture as "The collection of perceptions, attitudes, values , assumptions and knowledge that guides how things are done in organization in order to be consistent with the information security requirements with the aim of protecting the information assets and influencing employees' security behavior in a way that preserving the information security becomes a second nature". Information security culture changes over time [3].

In the case of information security management, changes will happen in technology, policy, procedures, and daily routine of how employees do their daily jobs and interact with the information assets. When there is change in the organization employees either: embrace it, fear it, or resist it [4]. Dealing with this change is a challenging task for the organization management and change agents who are responsible for establishing the information security culture as resistance and non-compliance from staff is a possible situation [5]–[8]. Researchers suggest that organizations benefit from IT initiatives most when it is supplemented by appropriate change management skills [9].

In the information security management domain, literature has included several frameworks, models and guidelines to guide organizations to establish and manage information security change. Nevertheless, very few have addressed the transition process towards achieving information security culture within an organization. a deep review of literature published between 2003 and 2013 indicates that 33% of 62 published papers in this domain suggested that incorporating change management could be considered as a major component in achieving an effective information security culture and to assist employees with the transition and to accept the new working polices [2]. It includes the work of [3], [6], [10]–[15].

However, examining these studies reveal that only two published papers in information security culture in a ten year period (2003-2013) have suggested some sort of guidance, namely Ngo et al.[6], and Okere et al. [7]. These papers have used some change management principles to support the establishment of information security culture. Nevertheless, these studies lack empirical findings to support their suggested programs. Table (1) summarizes the analysis of reviewed sources in that regard.

Table 1: Summary of the Analysis of the Literature Published During (2003-2013) In Information Security Culture in Regard Of The Use Of Change Management In Information Security Culture

Issue evaluated	Percentage of total
Recognize the need for Change management to achieve an information security culture	33%
Presented a Change management process to support the implementation of information security culture	3%

Resistance to change is expected, so the preparations must be substantially enough to help individuals realize changes to security behavior and attitude and interaction with information gradually. Using change management principles would help to overcome employees' experience of fear, shock, frustration and anger that may offer a fertile ground for insider information security threats [6]. In this context, we can define the change management as the act of managing modifications to an organization’s culture, behaviors and attitudes in order to achieve a desired information security culture.

Research is required to support management of how to implement the changes smoothly in the organization to achieve an effective information security culture, as the literature lack theories, models, and multistep approaches that should provide sufficient implementation guidance and support. The adoption of information security culture implementations from the perspective of change management has not been examined according to a recent study [2]. This presents a valuable opportunity for investigation.

This paper tries to answer the question: what are the major change management principles that could be used to build a sound information security culture? And how change management principles could be implemented within this context. In order to achieve that, this paper integrates a set of change management principles that were proposed in the literature and combine them to a comprehensive multistep framework that support and guide the transition in information security culture change within organizations. Moreover, the principles will be the base of suggestion of the appropriate guideline to support the effective implementation of change in information security culture among organization's members.

This paper is organized in the following order; firstly, this section introduces the problem and presents the research problem. Then, the existing change management approaches in information security are explored. Change management principles from different proposed principles and methodologies are combined and then mapped to information security culture related tasks. Finally, these tasks are combined to form the proposed information security culture change framework followed by a conclusion.

2. EXISTING CHANGE MANAGEMENT APPROACHES IN INFORMATION SECURITY

The literature review revealed that in the case of information technology related implementations, several change management approaches have been used successfully [4], [8], [16]–[18].

There are several guidelines and models that have been proposed in this domain, for instance, Kotter’s Eight-Step Model [8], Schein [19], and Ulrich’s Seven-Step Model. These models are summarized in Table 2.

Table 1: Kotter (1996); Schein (2009); Ulrich (1998) Models Of Change Managment

Schein (2009) Based on Lewin's Model (1951)	Ulrich's Seven-Step Model (1998)	Kotter's Eight-Step Model (1996)
Unfreeze (creating motivation for change through disconfirmation and psychological safety	Lead change	Establish a sense of urgency
Movement (learning new concepts and new meanings for old concepts through imitation of and identification with role models	Create a shared need	Form a guiding coalition
Refreeze (internalizing the new concepts and new meanings).	Shape a vision	Create a vision
	Mobilize commitment	Communicate the vision
	Change systems and structures	Empower others to act
	Monitor progress	Plan for and create short-term wins
	Make change last	Consolidate improvements and produce more change
		Institutionalize new approaches.

According to Harding [20] four key factors are behind the success when implementing change within an organization:

- **Pressure for change**: Recognizing the need and advantages of establishing an information security culture within the organization combined with senior management commitment is essential to successful change.
- **A clear, shared vision**: would benefits the whole organization where everyone is involved and participating as the information security is everyone responsibility
- **Capacity for change**: by making the resources available, this may include time and money for training and support.
- **Action:** through the cycle of "freezing, movement, unfreeze", and keeping the communication channels open

In spite of several theories, models, and multistep approaches, change in information security is usually hard to achieve as it requires the dealing with basic assumptions, tacit knowledge, values and beliefs. Organizational leaders lack a clear understanding of the steps necessary to implement change successfully [18]. Due to the lack of models and frameworks in information security culture change management, general approaches in information technology change management are still the main reference in information security culture change.

Williams & Williams [9] have offered a framework that was derived from a study of the change management literature. Their framework was designed to assist in understanding ICT investment initiatives through an evaluation process. The framework corresponding to a three-phase model of change implementation of Lewin's model (freezing, movement, unfreeze). The three stages in their framework are: Initiation, implementation and then institutionalization or continuation. They have discussed a number of major related issues, namely: communication, motivation, resources, championing and change agency, and project timescale.

Hornstein [4] discussed the use of change management to successfully implement IT programs. His discussion is based on Kotter's eight steps model that integrates leadership, empowerment and systems thinking. His paper talks about challenges to successful change and major success factors. He argues that effective change is mostly dependent on ensuring management support, organizational readiness, learning the organizational environment upfront, incremental successes and short wins, involvement of all stakeholders, training, and change champion(s) to support the change initiative.

Gilley et al. [18] developed a model that focuses on behaviors related to leadership effectiveness in change management. Organizational leaders may function as change agents to lead the change effectively. They suggested a number of independent variables that lead to successful change which are: Coaching, rewarding, communication, motivation, involvement of employees in decision making, and encouraging teamwork and collaboration.

Ngo et al. [6] discussed the transition process towards organizational change and proposes a transition model for information security culture change in SMEs. In their model, successful transition goes through three phases: (1) ending,

(2) neutral zone, and, (3) new beginning. These phases shall not be considered as separate stages with clear boundaries. At the beginning phase management shall persuade people to end the past and move on. Communication is an essential part at this stage to help people to change how they behave or react in a new and different manner. The neutral zone phase is the most complex and confusing phase in the transition phase. At this phase, managers should define the new requirements and guide their employees in the right direction. On the other hand, employees shall adjust to these requirements and start to take action to meet the requirements.

After that, the phases end with a new beginning of information security change. This includes reinforcing and committing to the new status quo for managers. The model is differentiating between two types of change players, namely, leaders and followers. Where leaders' role is overseeing and managing the process and the followers adapt and accept the transition. Each stage has different roles as the following figure summarizes it.

TIME

Change Player	Phase 1	Phase 2	Phase 3
	Ending	*Neutral zone*	*New Beginning*
Management **"Leaders"**	Communicate what has to be changed and reasons for change and the potential losses for whom	Define & Steer new requirements and what to do	Reinforce & Commit to new status quo
Employees **"Followers"**	Understand & recognize what has to be changed and reasons for change	Adjust to new requirements and take action	Accept & Embrace new status quo

Figure 1: Ngo et al. (2007) Information Security Culture Transition Model

During the three phases of transition, individuals go through different stages of psychological experiences. Authors claim that understanding these stages and how employees deal with the change can provide a strong reference for managers regarding how to lead and manage change. Authors have discussed a number of change management skills that facilitate the change, namely, top management support, learning, focus groups and workshops, redefining new requirements, establishing temporary solutions that allows for measurement and benchmarking, and communication.

Van Niekerk & Von Solms [21] have used a transformative change management process for the management of an information security culture change. Their focus was on using educational principles that contribute towards the establishment of an information security culture. The critique to their model is that it is dedicated to awareness and educational programs that aims at information security cultural change. Their focus was on using educational principles that contribute towards the establishment of an information security culture. The critique to their model is that it dedicated to awareness and educational programs that aims at information security cultural change. Their framework is represented in Figure 2.

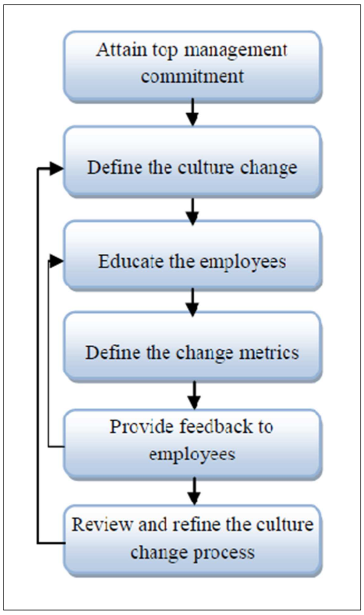
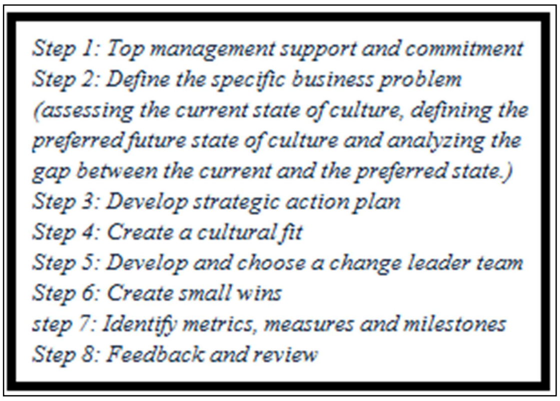

Attain top management commitment
Define the culture change
Educate the employees
Define the change metrics
Provide feedback to employees
Review and refine the culture change process

Figure 2: Van Niekerk & Von Solms (2005) Model

Okere et al. [7] presented a multistep guideline for information security culture. They have provided an assessment of the current information security culture approaches and focused specifically on the culture change process. Their culture change process is adopted from [21] and shown in Figure 3.



Step 1: Top management support and commitment
Step 2: Define the specific business problem (assessing the current state of culture, defining the preferred future state of culture and analyzing the gap between the current and the preferred state.)
Step 3: Develop strategic action plan
Step 4: Create a cultural fit
Step 5: Develop and choose a change leader team
Step 6: Create small wins
step 7: Identify metrics, measures and milestones
Step 8: Feedback and review

Figure 3 Okere et al. (2012) Information Security Culture Change Mangmnet Model

3. PRINCIPLES OF CHANGE MANAGEMENT IN INFORMATION SECURITY CULTURE

Critics of the previous mentioned models (Kotter, Schein, Ulrich) of change management refer to failure to recognize the human factor, and difficulty in following the rigid steps in order [18]. Therefore, researchers suggested a number of principles that could lead to effective change management in information security culture. Some of the principles were common across many studies.

Table 3 summarizes the main change management principles that were suggested by different studies in information systems-related change management. The inclusion tick (✓) is used to indicate whether the principle on the left column have been addressed by the specific study. The principles are listed without specific order. Also some may argue that overlapping might be evident like (management support and sufficiency of resources) and (training and focus groups). In fact, they have been separated to emphasize their importance.

Table 2: Principles Of Information Security Culture Change Management In The Literature

Change management principle	Gilley et al. (2009)	Hornstein (2008)	Williams & Williams (2007)	Ngo et al. (2005)	Okere et al. (2012)	Van Niekerk & Von Solms (2005)
Management support	✓	✓		✓	✓	✓
Sufficiency of resources		✓	✓		✓	
Analysis of the culture		✓		✓	✓	✓
Motivation	✓		✓			✓
Communication	✓	✓	✓	✓	✓	
Training	✓		✓	✓		✓
Change Agents	✓	✓	✓	✓	✓	
Focus groups and workshops		✓		✓		✓
Involvement and ownership	✓	✓	✓			
Success measures and milestones		✓		✓	✓	✓

The most common change management principles across models will form the basis of selection. The selection criterion was that the principle must be proposed by at least three studies out of the total selected studies. The principles are represented in Figure 4.

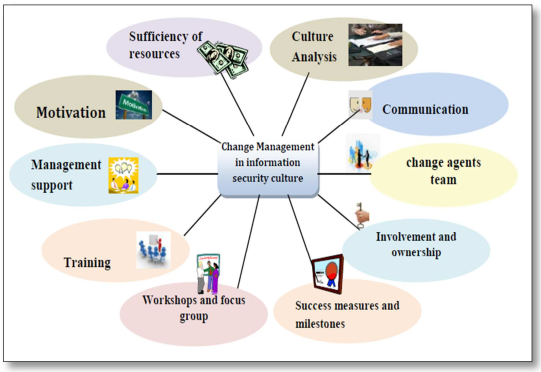

Sufficiency of resources
Culture Analysis
Motivation
Communication
Management support
Change Management in information security culture
change agents team
Training
Involvement and ownership
Workshops and focus group
Success measures and milestones

Figure 4: Information Security Culture Change Management Principles

These principles will be the base of suggestion of the appropriate guideline to support the effective implementation of change in information security culture that will be used to propose a multistep framework. In Table 4, each principle has been mapped to one or more tasks that will form the final multistep framework. In this table, the order of principles is important. A discussion for each step is provided afterward.

Table 3: Information Security Culture Change Management Guideline

Change Management Principle	Guide
Management support	Establish and gain a management support
Analysis of the culture	Revise existing organisational culture and process and identify what changes are required. Define clearly the steps required to get from the current state to the new desired state and gain management approval for them.
Change agents team	Select change agents team and encourage teamwork and collaboration.
Sufficiency of resources	Ensure the availability of the required resources such as time and money.
Communication	Communicate and sell the changes to all the stakeholders. Open different channels to facilitate the feedback and review.
Focus group and workshops	Establish focus groups and workshops.
Motivation	Motivate and empower the employees and monitor the motivation level among them.
Training	Coach and train employees to develop skills and knowledge base.
Involvement and ownership	Involve the employees in the decision making and mobilize the commitment. Enhance the sense of ownership and responsibility for the security of information assets.
Success measures and milestones	Identify small wins, measures and milestones to generate momentum and track the success of the change.

a) Establish and gain a management support

Top management support has been recorded as the most significant factor affecting information security management activities (Alnatheer et al. 2012). Top management shall show a commitment to information security and to information security culture. This should include developing vision and mission statements, slogans, and information policy changes. In addition, Management should make it clear to the organization members that security of information is essential in the organization.

b) Revise existing organisational culture and process and identify what changes are required

Management needs to understand the existing current state of culture and why change is needed. This step should include assessing the current state of culture including the current security related espoused values, artifacts and assumption. Interviews and surveys, might be used to in the assessment [21], [23]. Then, define the preferred future state of culture. After that, the gap between the current and the preferred state should be analyzed to determine what changes are required.

c) Define clearly the steps required to get from the current state to the new desired state and gain management approval for them.

The transfer steps from the current state to the required state should be clearly defined. This transfer could go through several intermediate states in some cases [21]. In this regard, Ngo et al.[6] model could be used to achieve that. The three major phases to change the culture are [19]: unfreezing, movement and learning, and finally internalizing/Refreezing.

d) Select change agents team and encourage teamwork and collaboration.

Change agent or change leaders are responsible for facilitating the change in the culture; they should be committed and competent. Change agents go through three stages. First, they formulate and sell a vision. Next they find power to advance their ideas. Finally, they must maintain the momentum. If the organization is large, then a change agent from different departments could be appointed. The change agents are accountable for facilitating the communication and feedback between top management and end users. Their role is to minimize confusion among employees to avoid their resistance and to prepare them for the effects of the change. Moreover, it is important to identify change champions who can influence others and act as role models [7].

e) Ensure the availability of the required resources such as time and money.

Before proceeding with the change in the culture, it is important to ensure that resource are identified, made available, and supported by top management. Shortage of any source could hinder the process and cause the interruption and lack of trust [20]. Resources may include time as well as money. Time is an essential resource that should be made available to the organization members who are targeted for the change. It is needed for training and in different security practices. It should also include training and support funding. Any required resource shall be clearly identified.

f) Communicate and sell the changes to all the stakeholders

Communication is essential to achieve a smooth and effective change. Change should be communicated to all staff in order to give them the opportunity to feed in their contributions, and the communication channels shall be made open and diverse. Ngo et al. [6] suggest that managers must take priority to communicate to their employees what has to be changed and the reason for information security culture change. This could help in relieving the stress and clarifying any misunderstandings as employees' understanding and recognizing of what has to be changed and reason for change it is crucial. Communication should also incorporate selling the required change to all the stakeholders who will eventually have to implement and work with it. Different methods could be used, for instance, posters showing the commitment of the organization to improving information security.

g) Open different channels to facilitate the feedback and review.

Continuous feedback is very essential to provide support, to avoid confusion, and to increase the involvement and ownership. It is considered as a driver for the desired cultural change [24]. Van Niekerk & Von Solms [21] argue that by offering the proper feedback mechanism, management is ultimately facilitating the implementation of the new security culture values by employees. Shared tacit assumptions are usually formed as the result of successful past behavior [25], therefore, it is important to provide feedback to employees and help them to recognize if their behavior is successful.

h) Establish focus groups and workshops

Focus groups and workshops are important to increase the user involvement process, and to enhance creativity and learning. Moreover, it allows managers and employees to discuss the transition and allow for questions and answers which could reduce confusion [6]. It could also be considered as a way to achieve the principle of training and awareness. However, for its value it has been separated as a single principle to emphasize on its importance. It allows employees to participate and contribute towards raising information security awareness among them and exchange knowledge and feedback.

i) Motivate and empower the employees and monitor the motivation level among them.

Employee's motivation plays a critical role in information security culture change management. Lacking suitable motivation, employees will only comply with guidelines that are aligned with their own tacit assumptions [15]. Motivation is essential in keeping the momentum of the employees to adapt to the new changes of how things are usually done. It is important to aid them to accept the change easily with the least possible resistance. It helps to raise the employees' appreciation of keeping the information secure by following the rules and adhering to security requirements.

Reward policy could include different methods, for instance, promotion, appraisal for good performance, and, peer recognition, etc. Moreover, Van Niekerk & Von Solms [21] suggested other ideas such as publishing monthly a summary of latest information security incidents in the organization, and providing clarifications of the possible consequences of these attacks if successful. In addition, it could include distributing information such as newsletters that reinforce the desired culture.

j) Train employees to develop skills and knowledge base

To ensure successful training, employees shall be educated on what to do, and how to do it, and also why it should be done [21]. Staff should be encouraged to develop their skills. Training will help raise the security awareness and decrease accidental or malicious threats to the information assets. Training should be done on continuous bases to improve the skills and knowledge base that each employee needs when handling information. Most employees are not aware of the information security risks that IT professionals are conscious of, even some straightforward ones. This emphasizes the need for raising the awareness among employees. Some researchers recommend that information security awareness programs should be presented to each new employee during the induction period. Moreover, new security risks appear every year, thus continuous efforts are required to help avoiding new risks. The interaction with IT systems should be as safe as possible to protect the information assets, lack of security awareness might cause risks to the safe interaction with information [1].

k) Involve the employees in the decision making and mobilize the commitment.

Employees' contributions through involvement are important to make them feel that they have joint ownership of the change that is being implemented. Employees shall be involved through different channels to increase their awareness and ownership. Employees should learn their responsibility in securing information assets [1]. Organization members should learn that they are responsible and liable for any security-related misdeeds and should be aware of the potential resulting consequences.

l) Identify small wins, measures and milestones to generate momentum and track the success of the change.

It is essential to identify small wins and actions that can be achieved towards the desired information security culture change [7]. These small wins would help to generate momentum and to keep up the motivation. In addition, different measures and indicators should be identified to track the success of the change. For example, identify a percentage of users who changed their passwords in one specified week. These measures and milestone will help to assess and judge the effectiveness of the processes.

4. FRAMEWORK OVERVIEW

In the previous section, information security culture change management principles have been combined from several proposed principles and approaches. A task or more have been presented for each principle. The proposed information security culture change framework will be based on combining the tasks together. In this section, a graphical description of this framework will be presented as in Figure 5.

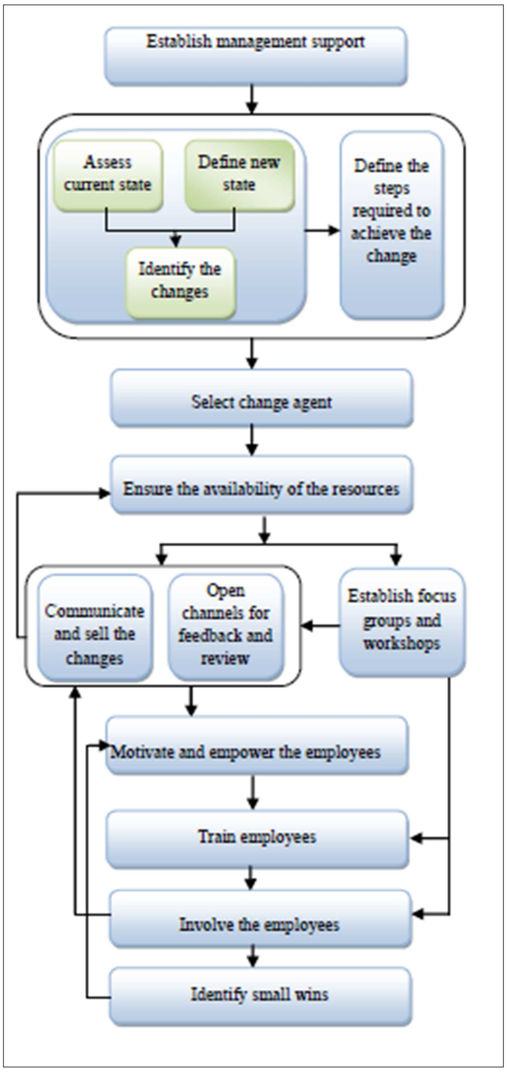

Establish management support
Assess current state
Define new state
Identify the changes
Define the steps required to achieve the change
Select change agent
Ensure the availability of the resources
Communicate and sell the changes
Open channels for feedback and review
Establish focus groups and workshops
Motivate and empower the employees
Train employees
Involve the employees
Identify small wins

Figure 5: Information Security Culture Change Framework

Arrows represent the sequence of performance of tasks. Some actions may be iterative, for example, feedback from end users may show the need for extra training, consequently the change leader need to go back into the step of checking the resources and then communicating to the employees. Focus groups and workshops as mentioned earlier will affect directly three principles, communication through review and feedback, training and awareness, and involvement. Therefore, three synchronous arrows are connecting it to the three tasks.

Identify small wins task has been connected back to motivation task. This is due to the fact that if employees have achieved the required metrics then they should be motivated through different reward suggested strategies. On the other hand, if not achieved, then other motivation strategies could be used, and this may require exposing the employees to extra training and awareness.

Involving the employees task usually result in getting feedback, consequently it has been connected to communication tasks through feedback and review.

The use of change management principles and the suggested framework would help organizations to achieve these benefits:

- Maximizing the information security culture benefits.
- Minimize the resistance to change among organization members
- Change agents will facilitate the communication and will help to provide the link between top management and staff.
- Smooth and successful implementation of information security culture and culture change.
- Allocation of required resources with right type, cost and effort to support the transition could be planned in advance.
- Increase the awareness and understanding among organization members and enhance their satisfaction and loyalty.
- Highlight management commitment, and increase collaboration across the organization departments.

5. CONCLUSION AND FUTURE WORK

The success of the establishing and managing the required information security culture is a team job; starting from top management and going down through the organization's structure to every single employee who interact with the information asset. However, changing employees' behavior to be consistent with information security principles and requirements in a way that information security becomes a natural aspect in the daily routine activities of every employee is not an easy job at all. It requires lots of efforts to change attitude, perception, routine and assumptions in addition to developing new skills and learning. Moreover, it will require the interruption to what employee is used to do.

A transition process is critical for successful information security culture change within organizations. It needs to be fully supported to ensure the minimum resistance and to avoid security risks to information assets throughout the transition period. This could be achieved through change management skills and principles. A number of available change management models and guidelines have been presented. However, very few have discussed the information security culture change.

The purpose of this paper was to highlight the main change management principles that were combined from several studies to be used in the field of information security culture. Moreover, it integrates the principles to propose a comprehensive guideline to support organizations in facilitating the transition in the culture. In addition, it proposes a multistep framework to help professionals and researchers to achieve a successful information security culture change within organizations.

We are planning in our future work to apply the framework to a case study to build strong evidence that the proposed framework can provide an added value to the strategies of implementing information security change. In addition, this proposed framework will be integrated with information security culture framework to propose a framework that enables practitioners to effectively establish information security culture within organizations.

ACKNOWLEDGMENT

The authors would like to thank Research Center in the College of Computer and Information Sciences, King Saud University for its support to complete this study

REFERENCES:

[1] A. Da Veiga, N. Martins, and J. Eloff, "Information security culture-validation of an assessment instrument," *South. African Bus. Rev.*, vol. 11, no. 1, pp. 146–166, 2007.

[2] A. Alhogail and A. Mirza, "Information security culture: a definition and a literature review," in *proceedings of IEEE World Congress On Computer Applications and Information Systems*, 2014.

[3] A. Da Veiga and J. Eloff, "A framework and assessment instrument for information security culture," *Comput. Secur.*, vol. 29, no. 2, pp. 196–207, Mar. 2010.

[4] H. Hornstein, "Using a change management approach to implement IT programs," *Ivey Bus. J. Online*, vol. 72, no. 1, pp. 1–8, 2008.

[5] S. Chang and C. Lin, "Exploring organizational culture for information security management," *Ind. Manag. Data Syst.*, vol. 107, no. 3, pp. 438–458, 2007.

[6] L. Ngo, W. Zhou, and M. Warren, "Understanding Transition towards Information Security Culture Change.," in *Proceeding of the 3rd Australian Computer,*

Network & Information Forensics Conference, Edith Cowan University, School of Computer and Information Science, 2005, pp. 67–73.

[7] I. Okere, J. van Niekerk, and M. Carroll, "Assessing information security culture: A critical analysis of current approaches," in *in the proceedings of IEEE conference on Information Security for South Africa (ISSA)*, 2012, pp. 1 – 8.

[8] J. Bennett, "Effectiveness Of Using A Change Management Approach To Convey The Benefits Of An Information Security Implementation To Technology Users, Unpublished PhD thesis," Capella University, 2012.

[9] M. Williams and J. Williams, "A change management approach to evaluating ICT investment initiatives," *J. Enterp. Inf. Manag.*, vol. 20, no. 1, pp. 32–50, Feb. 2007.

[10] T. Schlienger and S. Teufel, "Information security culture: from analysis to change," *South African Comput. J.*, vol. 31, pp. 46–52, 2003.

[11] C. Vroom and R. Von Solms, "Towards information security behavioural compliance," *Comput. Secur.*, vol. 23, no. 3, pp. 191–198, May 2004.

[12] M. Hentea, "A perspective on achieving information security awareness," in *Proceedings of InSITE2005: Informing Science + Information Technology Education, 16-19 June 2005.*, 2005.

[13] A. Ruighaver, S. Maynard, and S. Chang, "Organisational security culture: Extending the end-user perspective," *Comput. Secur.*, vol. 26, no. 1, pp. 56–62, Feb. 2007.

[14] S. Woodhouse, "Information Security: End User Behavior and Corporate Culture," in *7th IEEE International Conference on Computer and Information Technology (CIT 2007) 16-19 Oct. 2007*, 2007, pp. 767–774.

[15] J. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," *Comput. Secur.*, vol. 29, no. 4, pp. 476–486, Jun. 2010.

[16] S. Fulla, "Change Management: Ensuring Success in Your ERP Implementation," *Gov. Financ. Rev.*, vol. 23, no. 2, pp. 34–40, 2007.

[17] P. Legris and P. Collerette, "A roadmap for IT project implementation: Integrating stakeholders and change management issues," *Proj. Manag. J.*, vol. 37, no. 5, pp. 64–75, 2006.

[18] A. Gilley, J. Gilley, and H. McMillan, "Organizational change: Motivation, communication, and leadership effectiveness," *Perform. Improv. Q.*, vol. 21, no. 4, pp. 75–94, 2009.

[19] E. Schein, *The Corporate Culture Survival Guide*. San Francisco: Jossey-Bass, 2009.

[20] P. Harding, "Managing Change: A guide on how to manage change in an organisation," *Sustainable Business Department, Government Office for the South West*, 2004. [Online]. Available: http://www.oursouthwest.com/SusBus/mggchange.html. [Accessed: 01-Dec-2012].

[21] J. Van Niekerk and R. Von Solms, "A holistic framework for the fostering of an information security sub-culture in organizations," in *4th Annual ISSA Conference*, 2005.

[22] M. Alnatheer, T. Chan, and K. Nelson, "Understanding And Measuring Information Security Culture," in *Proceedings of the Pacific Asia Conference on Information Systems PACIS 2012*, 2012, p. paper 144.

[23] A. Martins and J. Eloff, "Information security culture," in *Security in the information society*, Boston: Kluwer Academic Publishers, 2002, pp. 203–214.

[24] J. Van Niekerk and R. Von Solms, "Establishing an Information Security Culture in Organisations: an Outcomes-based Education Approach," in *Proceedings of ISSA 2003:3rd Annual IS South Africa Conference*, 2003.

[25] J. Van Niekerk, "Fostering Information Security Culture Through Integrating Theory And Technology, Unpublished PhD Thesis," Nelson Mandela Metropolitan University, , South Africa, 2010.