Association for Information Systems
AIS Electronic Library (AISeL)

UK Academy for Information Systems Conference Proceedings 2012

UK Academy for Information Systems

Spring 3-27-2012

Measures for improving information security management in organisations: the impact of training and awareness programmes

Nesren Waly
School of Computing, Informatics and Media, Bradford University, nesreen_w@yahoo.com

Rana Tassabehji
School of Computing, Informatics and Media, Bradford University, r.tassabehji@bradford.ac.uk

Mumtaz Kamala
School of Computing, Informatics and Media, Bradford University, M.A.kamala@Bradford.ac.uk

Measures for improving information security management in organisations: the impact of training and awareness programmes

Nesren Waly, Rana Tassabehji and Mumtaz Kamala

School of Computing, Informatics and Media
Bradford University
United Kingdom
nesreen_w@yahoo.com; R.Tassabehji@bradford.ac.uk; and M.A.kamala@Bradford.ac.uk

Measures for improving information security management in organisations: the impact of training and awareness programmes

Abstract—**Security breaches have attracted corporate attention and major organisations are now determined to stop security breaches as they are detrimental to their success. Users' security awareness and cautious behaviour play an important role in information security both within and outside the organisation. Arguably the most common factor contributing to these breaches is that of human behaviour towards security, which suggests that changes in human behaviour can have an impact on improving security. One of the measures suggested to modify employee behaviour is through training and awareness-raising. However, before effective training and awareness programmes can be developed to achieve this aim, it is essential to understand what factors influence user behaviour and attitudes to information security. For this study, interviews with employees within the public and private sector were conducted to explore factors that influence security behaviour when using information. Our findings offer some preliminary recognition of implications for the designs of more effective training and awareness programmes that assure and sustain, in the long term, the appropriate behaviour towards security.**

***Keywords*—Information security, awareness, security behaviour, training and awareness programme, qualitative research.**

I. INTRODUCTION

Security breaches have attracted corporate attention in recent times as businesses are experiencing numerous challenges in managing information security. Considerable efforts have been made in recent years to examine the problem, and numerous security issues have been identified by existing studies to find the main reason for security breaches. However, most of these studies focus on the technical perspective rather than employee behaviour and performance. Human factors have been found to be responsible in 80-90% of organisational incidents, which highlights the behaviour of people in security breaches [1]. As users play a significant role in the information security performance of organisations, so their security awareness and behaviour becomes critical. Improvement in information security requires an understanding of what influences people's behaviour. According to many researchers, appropriate and positive human behaviour when working with computers represents the strategic key to the success of information security. Social psychology has been used successfully in changing the attitude and behaviour of people. This research would attempt to include behavioural principles in order to make security awareness programs more effective in addressing 'people's behaviour'.

The contribution of this paper is to explore and analyse the common factors that influence information security in terms of organisations, user behaviour and training, in an attempt to address and overcome the critical factors which may lead to security breaches in organisations. The following research questions are addressed in this paper:

1) What factors influence or cause information security breaches by employees in an organisation?
2) Can the behaviour of employees relating to information security be altered? If so, how?
3) Can information security management be improved through effective employee training?

The rest of the paper is structured as follows. First, a brief background and critical literature analysis is presented. Secondly, the research design is described, and finally, empirical results are presented and discussed and conclusion is presented.

II. LITERATURE REVIEW

A. Organisational factors

The world of information technology is constantly developing. Hence different types of technologies require different ways of improving security management to reduce security breaches. It is crucial for an organisation to understand the critical factors of information security. Indeed, the goal of information security is to protect the three major elements in IT: integrity, availability, and confidentiality within the system [2]. It supports the essential aspects of policy and how they should be continuously understood, communicated, and reviewed. There also appears to be a connection between the policy, people's awareness of it and the importance of educating users from all levels pertaining to the goals and the effectiveness of a successful policy. Compliance of policies is essential to make it effective; without enforcement a policy might as well not exist [3]. Roles and responsibilities are important factors that need to be each person's main priority from senior management to individual staff. This paper proposes that organisations cannot protect the three aspects of integrity, confidentiality and availability of information without ensuring that all employees and users have clearly understanding of their roles and responsibilities and are adequately trained to carry them out [4]. Therefore it is critical to provide knowledge of users' experience of information security and their specific security roles. Communication and documentation factors address the organisation's ability to ensure correct and secure operations. Meanwhile, incident response management to ensure the ability to take appropriate and complete action as quickly as possible in the event of any incidents is also critical.

Organisational factors such as policies, roles and responsibilities, communication, documentation, security awareness, risk management and incident response have the most effective information security management requirements that provide best practice and guidelines to reduce security breaches and improve employees' behaviour [5]. However, research proves that the main constraints regarding employees' roles in information security is their lack of motivation and knowledge regarding information security [6]. Furthermore, research also shows that a wide range of psychological, social, individual and cultural factors tend to affect the employee's behaviour in the organisation [7].

B. Behavioural Theory and Research

In the past thirty years, the theory of reasoned action (TRA) has been widely acknowledged as the major foundation of behavioural research. It proposed behavioural intention to perform or not to perform an action which is considered the immediate precursor to actual behaviour [8][9]. The theory of reasoned action introduced two factors that affect behaviour intention: attitude towards the behaviour and subjective norms. Attitude involves judgement as to whether the behaviour is good or bad and whether the person is in favour of or against performing it. The subjective norm is the awareness of how one should behave [8]. Ajzen extended his model and called it the theory of planned behaviour (TPB); he subsequently added another factor that influences behaviour intention - perceived behavioural control. This is described as the perception of how easy or difficult it would be to perform the behaviour [8]. Numerous studies use the model (of TRA and TPB) as the basis of their research in subjects such as class attendance [10], exercise and leisure activities [11][12]. It has also attracted the interest of many information systems researchers and has been observed as highly valid [13]. Findings from this research concluded that the best predictor of a person's behaviour is the intention to perform the behaviour. The theory of planned behaviour will be used in this study to identify the factors that influence user behaviour and assess how to accommodate these factors in information security management and implement an effective security awareness initiative.

C. Training and awareness

A review of prior literature reveals that many researchers have adopted different information security training techniques to address the elements that make up a successful information security awareness program, such as awareness, training and education. Others identify motivation as a successful way of promoting learning, performance and enjoyment [14]. Reward is also considered an essential element to improve security behaviour [15]. The problem with this factor is that people consider reward a motivation for behaviour; when this incentive is removed people may not sustain the appropriate behaviour, because the reason for performing the action no longer exists [16].

Empirical research [17][18] has found that the factors of self-efficiency, satisfaction and communication skills are the most cost-effective elements in terms of investing in workplace training. These three factors are critical to organisational performance and success after training. It was affirmed by [19][2l0] that training is increasingly being used to change and assist an organisation in achieving its strategic objectives. However, security breaches have attracted corporate attention in recent times as businesses are experiencing numerous problems in managing information security [21]. The evaluation of existing training programmes was carried out immediately after the implementation of the programmes; however, the long-term effectiveness of the training programme is still unknown. Therefore, to be able to achieve an effective training and awareness programme, training should incorporate a technique which ensures that appropriate changes in user behaviour are sustained in the long term.

III. RESEARCH METHODOLOGY

Qualitative research is used as an exploratory tool aimed at seeking insight and assessing phenomena in a new light. This approach will facilitate learning about the subject being investigated from different perspectives and to understand it in more depth. It is anticipated that the factors that cause organisational information security breaches can be identified, and what influences and impacts users' attitudes towards using computers, characterising the factors that affect user behaviour, which influences learning. Semi-structured interviews were conducted and the questions were divided into three sections. The first part was aimed at gaining insights into organisational factors related to information security management with a view to reducing information security breaches. The second part was aimed at exploring and testing the theory of reasoned action to understand and analyse people's attitudes towards using computers, concentrating on characterising the factors that affect user behaviour, which influences learning. The third part was aimed at exploring the impact of training and awareness programmes on security management behaviour.

IV. INTERVIEW METHOD AND ANALYSIS

Four organisations in the public and private sectors were chosen, and within each of those organisations ten interviews were conducted. Forty interviews were conducted lasting about an hour each. The different respondents provided different and detailed perspectives on information security issues and factors that influence their behaviour towards information security. The purpose of the study was clearly explained to each participant and confidentiality and anonymity were assured to ensure that the participant could speak freely without any concerns.

The interviews provided valuable insight into the issues under investigation. The themes that emerged are summarised, categorised and presented in the following tables and extracts from some of the contributions are also included.

A. First: employee's evaluation of their organisational information security polices

Interviewee's Comments	**Factors**
"organisation have policies with clear instructions on every single aspect of information security and how someone should be acting in facing any incident" *"all employees before they start the work have to read and sign the policy documentation".* *"policy needs to be presented in an attractive way, like image, and needs to be handed, emailed, displayed as screen saver, display it a card, on disc, and doors to remember it*	**Policy**
"connect their success with the success of the organisation" *"role model and sharing knowledge and experience"* *"Recognition and trust of employee's capability".*	**Motivation**
"the policy is not visible all the time, it is somewhere in a book in the drawer " *"the document is too big, there is no time to read all the policy and remember it all the time"* *"employees and end users are not aware of all the threat nor are they familiar with the possible consequences"*	**Lack of awareness**
"increase of workload will cause a conflict of interest between information security and functionality" *"information security is not their job, they don't consider it to be as their priority"* "*incidents that occur will be handled by security professionals and any losses will be replaced immediately"*	**Lack of clear roles and responsibility**
"we do not get any feedback and updates on such information security" *"we do not face and communicate with professional people and how they handle and recover any incident to be able to learn from them"* *"Expressing own ideas is always avoided".*	**Lack of communication and documentation**

"not trying to make an effort to comply with the policy of information security because there is no disciplinary strategy of reward and sanction procedure" *"fear level and the implication of the consequence is low"* *"They believe the cost of cautious behaviour is higher than the perceived benefits of cautions behaviour".*	**Lack of rewarding and sanction strategy**

The findings showed that employees ultimately feel that the organisation should have clear and concise policies/instructions on all aspects of information security and how users can effectively deal with incidents they may face. On the other hand, employees generally believe that information security is important to them and to their organisation so they are motivated to apply all the policies. However, there are some barriers to this.

Interviewees indicated that the policy is not visible all the time and is stored in some inaccessible location. This makes it difficult to remember the aspects of the policy and leads to poor management when an incident occurs. Individuals undertook very few of the information security actions as they claimed to have had no time to read all the policy and remember it. They are neither aware of all the threats nor familiar with the possible consequence of security breaches. Some of the interviewees indicated that an increase in workload will cause a conflict of interest between information security and functionality, as they believe the documentation is cumbersome and it is not possible to read it all. Some employees stated that information security is not their responsibility and they do not consider it to be their priority as they only have to concentrate on their own working task. Furthermore, they believe that the security is in place. At the same time they believe they are not required to carry out security tasks as they assume them to be the responsibility of designated security professionals who will handle the incidents and restore any losses immediately. Thus, the effectiveness of employees' roles and responsibilities and the power to reinforce information security actions by employees is lacking. In addition, the interviewees consider communication or the lack of it a barrier to complying with information security management. This signals the need/importance for sharing knowledge between employees and managers and increases the employee's involvement in avoiding and resolving security incidents. This will increase their capability and improve their self-efficiency to practise information security actions.

Others believe that, if users are too cautious about information security, it will be impossible for them to carry out their work smoothly. Finally, some indicate that there is a lack of clarity on the disciplinary strategy, as a reward and sanction system is not in place. Therefore, their apprehensions of the implications and consequences are at a low level, which leads to little effort being made to comply with the information security policy. Hence, the use of reward and sanction strategies leads employees and end users to participate more readily and make a concerted and persistent effort to work and achieve goals; these strategies also motivate them to be stronger when they encounter difficulties. The employees point out that examples of effective rewards could be bonuses, salary increases, praise, recognition from others, titles, certificates, new responsibilities, extended breaks, more flexible working hours, and gifts vouchers to show appreciation for their improvement and rectification of undesirable habits regarding information security.

Thus, the major factors found to influence information security in organisations are (1) lack of awareness; (2) lack of defining roles and responsibility; (3) lack of communication and documentation; (4) lack of reward and sanction systems; and finally (6) lack of reinforcement and practice. Considering these information security factors, it can be seen that people's information security behaviour is inadequate to effectively manage and reduce information security breaches.

B. Factors influencing user behaviour toward information security

TABLE II

Interviewee's Comments	Factors
"I believe the information security policy is very important to employees and to the company" *"There is no time available in the work place and we are too busy to think about information security".* *"We know all information security procedure and I think my behaviour is roughly the same as the documented information security policy behaviour.*	**Belief**
"we do not get any feedback and updates on such information security which lets us hypothetically think that we are working in the right manner and unfortunately the reminder toward information security will be quickly forgotten as it is not effective at all" *"the habit is affecting their attitude"* *"there is a fear to break the routine of doing something to respond to the situation in different way"*	**Attitude**
"environment and people around are not helping us to change" *"no observation, ineffective reinforcement and ineffective awareness procedure."* *"self-efficacy and engagement are helping us to diagnose and deal with information security to accomplish the goal of sustaining the information for longer"*	**Intention**
"to be able to change connect your task and goals with your success and dream" *"role model and sharing knowledge and experience"* *"connect the risk, the contemplation and the consequence to real life."*	**Motivation**
"stimulate the advantage and disadvantage, benefit, consequences of a behaviour" *"identifying clearly how and where to target strategies for changing behaviour"* *"explain in convincing techniques what is the problem and how to solve it"*	**Awareness**

Understanding the factors that impact user behaviour towards information security identifies how and where to target strategies for changing and improving people's behaviour and ability to maintain appropriate behaviour toward information security. [23] It is important to understand how people behave, as this knowledge assists in spreading information security consciousness and awareness.

The interviews revealed that belief is considered the most effective tool for influencing user behaviour. The habit attribute, which enables people to deal with any situations that they encounter without paying attention to the environment and the consequence of the behaviour, was also identified. The respondents believed the cost of cautious behaviour is higher than the perceived benefits of cautious behaviour. The interviewees believe that information security is very important to them and to the company; however, there are certain barriers which are not helping them to comply and sustain the security management behaviour. For instance, people stated that there is no time available in the workplace and they are too busy to think about information security. Several of the interviewees shared the belief that they know all the information security procedures and they think their behaviour roughly complies with the documented information on security policy behaviour.

However, this belief signals that people tend not to be completely sure about the established policy of information security as they think they are already acting in compliance with these policies. Other interviewees pointed out that they do not get any feedback and updates on such information security, which lets them believe that they are working in a secure manner. Unfortunately the reminders about information security will be quickly

forgotten as they are not effective at all. Hence, the pattern of not being familiar with the requirements and the misconceived belief that they are behaving in a secure manner is explained by: (1) lack of counselling; (2) lack of social support; (3) lack of feedback and assistance. Furthermore, not preparing employees to analyse their behaviour decisions and not helping them to engage in changing their procedures was considered a reason for employees failing to act securely. Overall, it was considered that the security management department should be visible to allow communication, share knowledge and best practice behaviour between employees, and update them frequently with effective reminders about standard rules of information security management. Employees' habits are also claimed to have a strong effect on their behaviour toward security. Their first response is that they are not well-informed on what security actions they should take. Secondly, they fear having to break work routines in order to respond to a new situation appropriately in different ways. Thirdly, the environment does not help them to change their habits, as there is a lack of observation, ineffective reinforcement and ineffective awareness procedures. Therefore, implementing reward and sanction processes increase interest, performance, motivation and improve users' behaviour towards security. These findings confirm other studies which find that, when behaviour is followed by a reward, it is considered a motivation stage and that behaviour is expected to be repeated in the future [24]. Finally, in order for security awareness programmes to add value to an organisation, it is necessary to highlight and emphasise user behaviour to measure its effectiveness.

C. Evaluation of the impact of training and awareness programmes on information security management behaviour

TABLE III

Interviewees Comments	**Factors**
"recognize the need and the importance of the knowledge" *"Making the effort to practise the skill and to attain the desired behaviour".* *"perceive the successful objective target all the time*	**motivation**
"there is too much information and too many rules which is leading to lack of communication and sharing knowledge between the participant and the instructor" *"no group discussion , no respect for individual point of view "* *"no participation and involvement and feedback from the trainer "*	**Lack of communication**
"Increase trainer goal to learn, trust their capability and praise their successes to encourage and build up their self-efficacy." *"build awareness, knowledge familiarity and consistence positive feedback when required"* *" emphasis on convincing rather than top-down persuasion*	**Self-efficacy and satisfaction**
"*too much information, no simplicity, not a lot of visualisation, descriptive image, group discussion and real example"* *"lack of engagement, reinforcement, hand s-on practice."* *"Need mixed type of approach of one training, include, presentation, practical, video, brainstorming, descriptive imaging and real example."*	**method of training**
"learning environment needs to be more convenient and involve more practical to allow the reinforcement of the learning to improve the job performance" *"attract people attention to motivate them to make extra efforts to improve their performance, such as colours, consistence, simplicity, discussion, help and support and attracted navigation"* *"Quizzes and self-assessment strategy to gain attracted.*	**human computer interaction**
"monitoring, observation and assessment will help reinforcement of the leaning" *" preparation ,effort and action to practices all the time"*	**Reinforcement**

"control and maintenance the learning to overcome and achieve the learning behaviour."	
"Determine what the participant needs" *"clearly select the objective goals that aimed to which is satisfying the participant needs"* *"Choose appropriate training method to solve problem, to change attitudes, and to reinforce to practise the skills."*	**Awareness**

This section investigates and identifies the characteristics of effective training, to help people retain security information for longer and persistently improve their performance on information security. In order to provide effective training, firstly it is essential to think broadly and deeply about how users will contribute to sustain the appropriate behaviour. Secondly, it is necessary to focus on the factors of training and awareness programmes that impact on information security management behaviour.

The most essential factor of learning was found to be motivation, which includes recognising the need for and the important of knowledge and making the effort to practise and maintain the skills to attain the desired behaviour. Most of the interviewees are motivated to learn and to gain knowledge to be able to maintain, to manage and to apply the appropriate information security behaviour.

However, there are certain barriers regarding training programmes that need attention to help users comply and sustain good information security. Interviewees indicated that there is a huge lack of user involvement and user participation in training programmes. There is too much information and too many written rules in the documentation which has led to a lack of communication and sharing of knowledge between the participant and the instructor. Therefore, it is essential to allow the users to participate, to present their opinions and to share their experience as part of the learning process. These are considered effective approaches for improvement of information security knowledge and awareness. Other interviewed users stated that, when developing training programmes, it is important to take into consideration different adult learning styles to attract people's attention, such as using videos, animation, examples from real-world scenarios, descriptive images, and minimising the amount of information to give users a chance to think differently. Other interviewees point out that, although there is information available from a variety of sources including the Internet, books and hand-outs, they were not actively seeking knowledge on information security as they point out that there is a lack of engagement, reinforcement, hands-on practice and an engaging method of training. This signals the importance of self-efficiency to increase participants' motivation to learn, and help them to understand, diagnose and deal with day-to-day problems to accomplish the goal of retaining the information for longer and complying with good behaviour practices. Self-efficiency allows employees and end users to be satisfied with their work, and motivates them to make an extra effort which leads to better performance in the work environment. Interviews with employees and end users revealed that the reason for them not retaining the information for longer is that there appears to be only one method of training. For example, there is too much information and a lack of simplicity; there is also a paucity of visualisation, descriptive images, group discussions and real examples. This shows the importance of interactivity in the learning process as a convenient and practical method of training, thus allowing employee satisfaction and reinforcement of the learning to improve performance.

Finally, to make training programmes more effective, it is essential to integrate all the influential factors of training, including organisational factors, human behaviour factors and training effectiveness factors, in order to build up a foundation for effective training outcomes. Swanson and Wang [25] highlighted that, if the training programmes are not linked to organisational goals and strategy, they are unlikely to produce a performance that is recognisable by the organisation.

Table 4 shows the frequency of the themes mentioned by respondents. This crudely shows that reinforcement and reward are very important as they are mentioned by all users. Factors such as awareness, sanctions and motivation communication are also important and actively encouraged in order to ensure compliance by the employees.

TABLE IV: F*inal interview result*

interviewer	orgnsation factors						user behavior factors						effective traning factors					
	awarness	policy	role	responsibility	communicaation	documentation	rewarding	sanction	motivaiton	believe	attitude	intention	motivaiton	awanress	reinforcement	communcaiton	self-efficacy	method fo traning
40	35	29	12	18	30	24	40	37	36	28	15	13	35	38	40	35	30	25

V. CONCLUSION

The world of information technology is constantly developing and evolving. Hence different types of technologies require different ways of improving security management (to reduce and mitigate security breaches). The literature review reveals that users and awareness factors are considered the most important means of enhancing and improving information security. The result of this study has identified the factors that were consistently significant in affecting information security breaches in (organisation factors, user behaviour and training factors) such as awareness, motivation, communication, reinforcement and reward and sanction factors. Aiming to concentrate on retain security information for longer and persistently improve their performance on information security

In addition, based on gathered sources of evidence, the authors believe that to achieve the effectiveness of training and awareness programme, it is highly suggested to understand what factors influence user behaviour and attitudes to information security to be able to modify employee behaviour through training and awareness-raising.

VI. REFERENCES

[1] J.T. Reason and A. Hobbs, *Managing maintenance error: a practical guide*, Ashgate Publishing, 2003.

[2] G. Stoneburner, et al., "Risk management guide for information technology systems," *Nist special publication*, vol. 800, 2002, pp. 30.

[3] K.J. Knapp, "Information security policy: An organizational-level process model," *Computers & Security*, vol. 28, no. 7, 2009, pp. 493-508.

[4] M.E. Whitman, "In defense of the realm: understanding the threats to information security," *International Journal of Information Management*, vol. 24, no. 1, 2004, pp. 43-57.

[5] S. Sowa, et al., "BORIS–Business ORiented management of Information Security," *Managing Information Risk and the Economics of Security*, 2009, pp. 81-97.

[6] M. Soliman and L. Lapointe, "Motivational Needs And It Acceptance: The Need For A Richer Conceptualization Of The Perceived Usefulness Construct," ref 2009..

[7] P. Taylor Gooby and J.O. Zinn, "Current directions in risk research: New developments in psychology and sociology," *Risk Analysis*, vol. 26, no. 2, 2006, pp. 397-411.

[8] I. Ajzen, "The theory of planned behavior," *Organizational behavior and human decision processes*, vol. 50, no. 2, 1991, pp. 179-211.

[9] L.N.K. Leonard, et al., "What influences IT ethical behavior intentions--planned behavior, reasoned action, perceived importance, or individual characteristics?," *Information & Management*, vol. 42, no. 1, 2004, pp. 143-158.

[10] I. Ajzen and B.L. Driver, "Application of the theory of planned behavior to leisure choice," *Journal of Leisure Research*, 1992.

[11] Y. Theodorakis, "Planned behavior, attitude strength, role identity, and the prediction of exercise behavior," *The Sport Psychologist*, 1994.

[12] G. Godin, et al., "The pattern of influence of perceived behavioral control upon exercising behavior: an application of Ajzen's theory of planned behavior," *Journal of Behavioral Medicine*, vol. 16, no. 1, 1993, pp. 81-102.

[13] K. Mathieson, "Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior," *Information systems research*, vol. 2, no. 3, 1991, pp. 173.

[14] P. Birjandi and N.H. Tamjid, "The Role of Self-assessment in Promoting Iranian EFL Learners' Motivation," *English Language Teaching*, vol. 3, no. 3, 2010, pp. P211.

[15] P. Puhakainen, "A design theory for information security awareness," *University of Oulu*, 2006.

[16] C.I. van Wijhe, et al., "Understanding and Treating," Risky Business: Psychological, Physical and Financial Costs of High Risk Behavior in Organizations, 2010,pp. 107.

[17] R.A. Abiodun, *Leadership Behavior Impact on Employee's Loyalty, Engagement and Organizational Performance: Leadership Behavior and Employee Perception of the Organization*, AuthorHouse. 2010.

[18] S. Bährer-Kohler and E. Krebs-Roubicek, "Chronic Disease and Self-Management—Aspects of Cost Efficiency and Current Policies," *Self Management of Chronic Disease*, 2009, pp. 1-13.

[19] A.M. Saks, et al., *Managing performance through training and development*, Nelson Education, 2009.

[20] N.F. Doherty, et al., "Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy," *International Journal of Information Management*. 2010.

[21] C. Onwubiko and A.P. Lenaghan, "Challenges and complexities of managing information security," *International Journal of Electronic Security and Digital Forensics*, vol. 2, no. 3, 2009, pp. 306-321.

[22] K. Malterud, "Qualitative research: standards, challenges, and guidelines," *The Lancet*, vol. 358, no. 9280, 2001, pp. 483-488.

[23] V. Mahabi, "Information Security Awareness: System Administrators and End-users Perspectives at Florida State University". 2010.

[24] B. Bulgurcu, et al., "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *Mis Quarterly*, vol. 34, no. 3,2010, pp. 523-548.

[25] E. B. Swanson and P. Wang, "Knowing why and how to innovate with packaged business software," *Journal of Information Technology*, vol. 20, pp.20-31, 2005.