African Journal of Business Management Vol. 5(26), pp. 10862-10868, 28 October, 2011
Available online at http://www.academicjournals.org/AJBM
DOI: 10.5897/AJBM11.067
ISSN 1993-8233 ©2011 Academic Journals

Full Length Research Paper

Effectiveness of information security awareness methods based on psychological theories

Bilal Khan[1], Khaled S. Alghathbar[1, 2], Syed Irfan Nabi[1,3] and Muhammad Khurram Khan[1]*

[1]Center of Excellence in Information Assurance, King Saud University, Saudi Arabia
[2]Department of Information Systems, College of Computer and Information Sciences, King Saud University, Saudi Arabia.
[3]Faculty of Computer Science, Institute of Business Administration (IBA), Karachi, Pakistan

Accepted 24 March, 2011

Effective user security awareness campaign can greatly enhance the information assurance posture of an organization. Information security includes organizational aspects, legal aspects, institutionalization and applications of best practices in addition to security technologies. User awareness represents a significant challenge in the security domain, with the human factor ultimately being the element that is exploited in a variety of attack scenarios. Information security awareness program is a critical component in any organizations strategy. In contrast to other information security awareness work which mostly explains methods and techniques for raising information security awareness; this paper discusses and evaluates the effectiveness of different information security awareness tools and techniques on the basis of psychological theories and models. Finally, it describes how to measure information security awareness in an organization.

Key words: Information security, awareness, effectiveness, psychological, management.

INTRODUCTION

Information is one of the resources that an organization is heavily dependent on. If the critical information of an organization is compromised, the organization can suffer serious consequences, that is, in the form of loss of income, loss of customers' trust and maybe legal action etc. Therefore, information should be protected and secured.

Information security awareness is about guaranteeing that all employees are aware of the rules and regulations regarding securing the information within organization. Information security awareness should therefore form an integral part of any organizations' overall information security management plan.

Many organizations use readymade information securtiy awareness tools developed by some of the international information security companies, whereas some organizations make their own awareness tools according to the needs of the organization.

By implementing information security awareness program, it is not guaranteed that every audience have understood and obeyed the guidelines, therefore, it is necessary to measure how much a particular method is effective in fulfilling its purpose.

Related work

Kruger and Kearney (2006) developed a prototype model for measuring information security awareness in an international gold mining company. They measured the effectiveness of information security awareness program on the basis of knowledge, attitude and behavior. However, their research lacks the study of the underlying theory of the model.

Hagen et al. (2008) conducted research by analyzing answers of research question from 87 information security managers in Norwegian organizations. Albrechtsen and Hovden (2010) described 'information security dialogue' as an effective tool for increasing awareness, however, the study lacks the fact that how effective is

*Corresponding author. E-mail: mkhurram@ksu.edu.sa.

Abbreviations: **KAB,** knowledge-attitude-behaviour; **TPB,** theory of planned behavior; **TRA,** theory of reasoned action; **CBT,** computer-based training.

Table 1. Information security awareness methods effectiveness.

S/No.	Tool and technique	Component of knowledge	Component of attitude change	Component of subjective norms	Component of Intention	Change in behavior	Overall effectiveness
1	Education presentation	✓	✓	×	✓	✓	4
2	Email messaging	✓	✓	×	✓	×	3
3	Group discussion	✓	✓	✓	✓	✓	5
4	Newsletters	✓	✓	×	×	×	2
5	Video games	×	✓	×	✓	×	2
6	CBT	✓	✓	×	×	×	2
7	Posters	✓	✓	×	×	×	2

their approach as compared to other approaches of awareness.

According to Levin and Klev (2002), for a successful organizational learning, a change and development employee's participation and collective reflection are very important.

In order to increase awareness level, knowledge should be given to the audience as stated by Forcht, education is necessary for increasing user's ethical awareness (Forcht 1988). In addition, for the protection of critical information assets security education campaign helps changing manager's and employee's attitude and behavior (Wilson and Hash, 2003).

Although research has been done in the area of information security awareness, however the literature lacks the study on the effectiveness of information security awareness methods on the basis of psychological theories and does not describe the underlying theory of these methods. Psychology is the science of mind and behavior. Social psychology has been used for many years for research in the area of education, learning and human behavior. In this paper, we evaluate the effectiveness of each tool and technique on the basis of our proposed model which is the integration of knowledge-attitude-behaviour (KAB) model (Baranowski et al., 2003) and theory of planned behavior (TPB) (Fishbein and Ajzen, 1975).

RESEARCH DESIGN AND METHODOLOGY

Information security awareness can be defined as the individual's passive involvement and increased interest towards certain issues and it is considered one of the key components of consciousness-raising the other being action (Namjoo et al., 2008). According to information security forum (2003), information security awareness can be defined as the extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organization, their individual security responsibilities, and acts accordingly. Different researchers have defined information security awareness; however, this study is based on the definition done by Information Security Forum (2003).

Many information security awareness interventions are based on KAB model which mainly focuses on the knowledge aspect of the human being (Kruger and Kearney, 2006; Baranowski et al., 2003). According to KAB model, as knowledge accumulates in a relevant behavior, for example, information security, health, environment, education etc., changes in attitude are initiated. It basically explains the role of knowledge in the behavior change and the accumulation of knowledge. Such accumulation of knowledge in KAB model leads to change in attitude and finally behavioral change. Research in healthcare (Baranowski et al., 2003) and environmental awareness (Newbould and Furnell, 2009) shows that knowledge can be integrated in other conceptual framework in order to understand the process of change, but increase in knowledge is not the ultimate factor of change in behavior. It means that more than one variable affect behavior. Thus, the KAB model, by itself is not sufficient to bring change in attitude and behavior for long term. In order to understand the change in attitude and behavior and how a change in attitude leads to change in behavior we borrow the support of the theory of reasoned action (TRA) or TPB (Fishbein and Ajzen, 1975). This theory explains relation between attitude and behavior and includes both the direct attitude-behavior path as well as an indirect attitude-intention-behavior path (Farrior, 2005; Fishbein and Ajzen, 1975).According to the theory of planned behavior, the change in behavior depends on the intention of the person. There are two factors that influence intention. One factor is attitude and the other is subjective norms (Farrior 2005). So the level of intention towards an action will be higher if the person has a more positive attitude and more of a subjective norm towards the behavior. The attitude is what the person likes or dislikes whereas subjective norm is the person's belief what people think about him should be done. These two factors together cause intention which leads to change in behavior. To evaluate the effectiveness of information security awareness interventions, we propose a five step stair model. These steps are knowledge, attitude, normative belief, intention and behavior, where knowledge is considered as the foundation pillar of the model. Our proposed model takes the knowledge attribute from the KAB model, attitude and social norms from the theory of planned behavior to achieve the desired change in behavior. Table 1 lists three information security methods from formal and four from informal instruction methods (Hubbard, 2003) and shows their respective

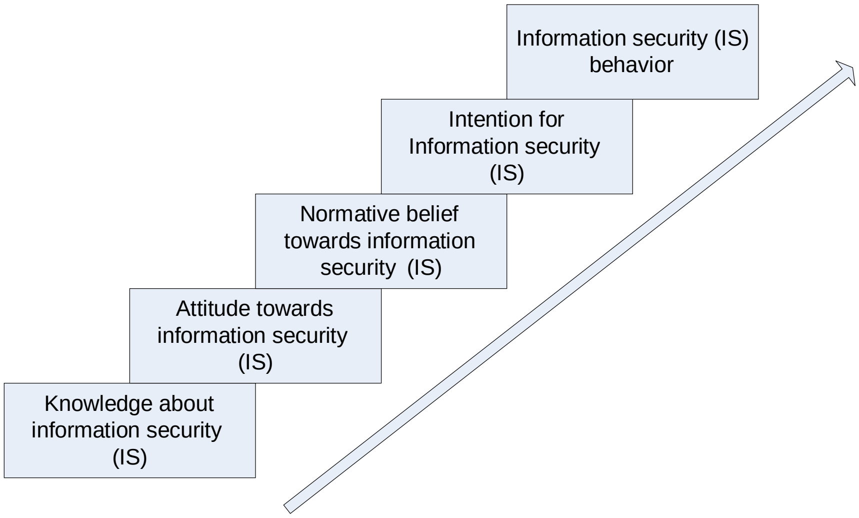
Information security (IS) behavior
Intention for Information security (IS)
Normative belief towards information security (IS)
Attitude towards information security (IS)
Knowledge about information security (IS)

Figure 1. Five step ladder model for measuring information security awareness.

effectiveness in the form of 5 points Likert scale, where 5 being most effective and 1 being less effective. In Table 1 the tick or 'x' mark below each component indicates its presence or absence in the respective information security awareness campaign. The overall effectiveness of a campaign method can be found by counting the number of tick marks in the respective campaign method. The more an information security awareness method contains elements from the model, the more it will be considered effective in raising the awareness level.

EFFECTIVENESS OF INFORMATION SECURITY AWARENESS TOOLS

As we have formulated how to measure the effectiveness of information security awareness methods, now we will find out the effectiveness of the following methods:

1) Educational presentation
2) E-mail messaging
3) Group discussions
4) Newsletter articles
5) Video games
6) Computer-based training (CBT)
7) Posters

Educational presentation

Behavior change objectives refer to intended changes in audience's actual behavior. Campaigns and behavior change objectives, together contribute to the overall program objective which refers to awareness. Education is often seen as the key to changing behavior. Different types of awareness campaigns are based on different psychological theories that focus on different aspects of human psychology. Usually the education campaigns target the knowledge aspect of the human and it ignores the motive behind the human behavior. Knowledge is not the motive for the human information security behavior; however, the lack of knowledge is a barrier in developing a desired behavior. In educational information security awareness campaigns, information is provided to the audience. Therefore these campaigns are mere the source of transfer of information and knowledge from the presenter to the audience. For example, information security awareness presentations provide information regarding password management, email management, virus protection, and organization's information security policies.

Although this is very useful information but increase in information does not lead to a change in behavior and awareness. Social norms which are more effective in causing intention are missing in presentation. In addition, these campaigns are cheap, but boring and ineffective.

Now comparing the components of presentation with our proposed model (Figure 1), it is clear that information security awareness presentations are more informative and provides more knowledge, therefore they can change the attitude but due to the missing component of subjective norms the component of intention of the audience remains unchanged. Therefore the overall effectiveness of information security awareness presentation is 4 points as shown in Table 1.

E-mail messaging

One type of campaign for information security awareness is email messaging. These messages disseminate useful information regarding phishing, social engineering, password management and information security incidents. This method is effective in providing security related related information and hence increases information security knowledge of the recipient. However, reading email message does not mean the message has been understood and internalized. Therefore, this method is insufficient in changing the attitude of the employee as this is one way communication and may not catch the attention of the recipient.

Using E-mail messaging for information security awareness is good in providing information and knowledge. This method catches attention but cannot change the behavior therefore effectiveness stops on the second step of the model (Figure 1), that is, the overall effect of this method in raising information security awareness is only 3 points as shown in Table 1.

Group dialogue

One type of information security awareness intervention is an informal meeting in which there is no one way communication. In this meeting, about 15-20 individuals of an organization participate and the participants take full advantage of sharing knowledge and experience (Albrechsten and Hovden, 2010). Different information security key issues are picked one by one and discussed; all participants are given equal opportunity to explain his point of view. In addition, organization policy regarding information security is discussed.

Participants are asked to describe any information security incident happened with them and whether those incidents were reported. The consequences of such security incidents are discussed among the participants. Such strategy of discussing incidents in workshops is good to motivate the participants. This strategy is based on the theory of reasoned action, which changes intention by changing attitude and social norms. Group discussion involves participants in conversation that increases the information security related attention and intention of the participants (Albrechsten and Hovden, 2010). Group discussion and meetings are more of interactive type and hence more effective.

This approach has been found useful in increasing the awareness level by the use of knowledge, attention, attitude, social norms, motivation and behavioral strategies. This approach uses social norms and interaction that influence individual's understanding of information security.

In addition, it is interactive and engages all the participants. Due to the ideal environment participants come to know about information security attitudes of each other and therefore increase their motivation to adopt positive information security behavior. This method of intervention accumulates all components of our proposed model (Figure 1) and therefore the overall effectiveness of information security group dialogue is 5 points (Table 1).

Articles in newsletters

Newsletter is a monthly or quarterly one to four pages information security report. These reports can be both in electronic or print format. They are distributed among The employees within organization and are designed with the aim to increase employee's information security awareness. It has a company logo on it with the date on which the newsletter was issued. The newsletter discusses the new emerging threat, for example, newly discovered viruses, computer security incidents and useful guidelines to overcome such incidents. These newsletters are good in transferring information security knowledge. They are also very informative and knowledgeable material due to which they are good in changing attitude towards information security awareness.

However, it is not possible for the security managers to know whether the employees have read the newsletter and they have understood and internalized it or not. In addition, it does not have the component of subjective norms, due to which it cannot change the reader's intention and so behavior. Therefore, the overall effectiveness of information security newsletters, according to our proposed model is only 2 points on a five-point Likert scale.

Video games

Some information security awareness researchers have proposed the use of video games to increase information security awareness (Newbould and Furnell 2009; Benjamin et al., 2006). This technique is also used by researchers in other domains to increase health (Baranowski et al., 2008; O'Connor et al., 2001) and environment risk awareness (http://triangleairawareness.org/p=55 and http://captaind-pc-aming.blogspot.com/2010/01/quit-smoking-with-help-of-video-games.html). It is claimed by the researchers that video game is a good technique in motivating player towards adapting the desired behavior as it catches the player's attention and engages him. However, this method does not have a component of knowledge transfer unless the player has already gained the information security knowledge before starting the game. In addition, it is related to information security in general and does not specifically reflect the policy of the organization or organization's related security issues. In our proposed model, knowledge is the foundation pillar for the increasing information security awareness and behavior.

Video games are more interactive and keep the player engaged. They are beneficial in changing attitude; however, they are not a very good source of knowledge. Due to which they lead to a very limited change in behavior therefore the overall effectiveness of video game on one's information security awareness is only 2 points.

Computer-based training (CBT)

Computer based training has several advantages over conventional methods of information security awareness. CBT is available at all times to all employees within the organization and it is an effective method of information security awareness training. The employees of the organization can acquire the desired training at their own pace. However, CBT requires more resources and do not reflect the organization’s policies. They are readymade. In addition this method lacks the benefit of interaction between instructor and audience and among the group of audience. Therefore, a social norm which is one of the components of our proposed model is missing in this method. Due to the missing component of social norms human’s information security intention and behavior does not change and therefore, the overall effectiveness of CBT is 2 (Table 1).

Posters

Posters are simple and effective reminders of information security that catches end user attention and reminds basic information security rules. Posters require fewer resources. Catchy slogans and attractive designs greatly contribute to the effectiveness of posters. In addition to the design and contents of the posters, location where the poster is displayed also attracts the attention of the viewer. Posters displayed in high traffic area are more likely catch the attention of the viewers.

However, relying on information security awareness posters alone is impractical as it is not possible to explain something on posters. In addition, a social norm which has a great contribution in raising awareness is missing in information security posters. Due to the missing component of social norms, intention cannot be changed and therefore, information security related behavior remains unchanged. Hence the overall effectiveness of posters is only 2 as shown in Table 1.

Comparative study of the effectiveness of information security awareness tools

Previously, the effectiveness of several information security awareness campaigns have been measured one by one based on our proposed model (Figure 1). The overall effectiveness of each of them is shown in Table 1. The most effective of them is information security related group discussion. It considers all components of the proposed model namely knowledge, attitude, social norms and intention. Information security awareness presentations are the second most effective method for increasing awareness as shown in Figure 2. E-mail messaging is the third effective method whereas newsletters, video games, CBT and posters are fourth effective methods for increasing information security awareness.

Information security awareness metrics

According to Wilson and Hash (2003) and Swanson et al. (2003), metrics is defined as tools to facilitate decision making, improve performance and accountability and help determine an organization’s information technology (IT) security awareness and training. Information security managers need methods to measure the information security awareness level of employees of their organization. A thorough literature review as failed to provide a universally accepted and validated measure of information security awareness. Here, we present the methods to measure the information security awareness.

Security related helpdesk calls

Information security awareness of employees can be measured by counting security related calls to helpdesk. However, the type of calls to the helpdesk varies and therefore every call to the helpdesk cannot be considered to measure awareness. For example if the calls are for resetting the password to unlock the account then this is due to the ignorance of the user. But if an employee or customer calls helpdesk for the advice regarding choosing password then it is counted in measuring information security awareness level. The more the number of such calls to helpdesk the more the level of information security awareness in the organization.

Accesses to unauthorized online services

Some organizations do not allow the use of certain online services which are not relevant to the organization’s business. With the use of automated tools it is possible to find out the number of attempts made to access those unauthorized services. Such measurement can be done monthly or quarterly, depending on the information security management policy of the organization.

Accesses to information security intranet pages

Many organizations create informative websites for the purpose of information security awareness training of the employees. Employees are instructed to visit those pages for the information security awareness training. The gradual increase in the number of hits to the website shows an increased interest of employees in information security awareness. The number of hits means the number of users being exposed to the information security awareness material. Therefore, the more is the number of hits, the higher will be the level of awareness.

Survey questionnaires based on knowledge

A survey based on information security questionnaire can be conducted within the organization among the employees. Unlike other types of measure this survey assesses, the knowledge of the employees about

Table 2. Information security awareness metrics.

Metrics	Unit
Security incident database	Incidents/6 months
Help desk calls	Calls/month
Phishing e-mails	E-mail/month
Number of accesses to intranet pages	Hits/month
Number of accesses to unauthorized pages	Attempts/month
Survey questionnaires based on knowledge	Average score of all employees

information security which indirectly measures the information security awareness level. Such surveys include questions: How to make a strong password? Is it secure to open an e-mail from unknown sender? Is leaving the system unlocked safe? Or do you lock the system before leaving? Such type of survey has many advantages and gives a clear whether the employees have knowledge about information security. Thus an increase in the number of correct answers of the survey shows an increase in the level in information security awareness. Such survey can be conducted monthly or quarterly depending on the policy of the organization to measure the level of information security awareness within organization.

Phishing e-mails

It is beneficial to find out the number of phishing e-mails that have been opened by the employees of the organization. The number of phishing e-mails accessed shows the level of information security awareness. The more is the number of phishing e-mails accessed, the less the level of awareness. Information security conscious users will less likely access suspected phishing e-mails. Such information can be collected either by asking employees whether they have received any phishing e-mails in a specified period of time or using an automated tool.

Security incident database

Information security awareness can also be measured by counting the number of security incidents being reported. It also indicates the awareness of the user who knows the person to contact when an information security incident occurs. Therefore, increase in the number of reported incidents as compared to the number of unreported incidents shows the increase in the level of information security awareness.

In addition to the above strategies, the statistics of increase and decrease in the number of Trojan horse attacks and analysis of log files of intrusion detection system can assist in measuring the information security awareness.

Table 2 shows two columns, a metrics column and a unit column. Unit describes the unit of the corresponding metrics which has been discussed above one by one. The table helps in measuring the information security awareness in an organization if the above measures are considered.

CONCLUSION AND FUTURE WORK

This research is a theoretical study of information security awareness based on the psychological theories of awareness and behavior. The study shows that psychological theories of education, learning, environmental and healthcare behavioral change can be used to make information security awareness methods more effective. It further clarifies that the aim of many information security campaigns is to increase information security knowledge. Many post-campaign surveys ask questions focusing mainly on the knowledge of the participant and do not assess user’s information security behavior. Answering questions correctly does not mean that the user is motivated to behave according to the knowledge they gained during the campaign. Information security awareness campaigns based on the proposed model have the ability to change user’s behavior and hence raise user’s information security awareness.

REFERENCES

Albrechsten E, Hovden J (2010). Improving information security awareness and behavior through dialogue, participation, and collective reflection. An intervention study. J. Comput. Secur., 29(4): 432-445

Benjamin D, Michael F, Cynthis E, Thuy D (2006). Cyber security training and awareness through game play. IFIP Int. Fed. Inform. Process., 201: 431-436

Baranowski T, Cullen KW, Nicklas T, Thompson D, Baranowski J (2003). Are current health behavioral change models helpful in guiding prevention of weight gain efforts? Obes. Res.. 11(10):23–43.

Baranowski T, Buday R, Thompson DI, Baranowski J (2008). Playing for Real: Video Games and Stories for Health-Related Behavior Change. Am. J. Prev. Med., 34(1):74–82.

Farrior M (2005). Breakthrough strategies for engaging the public: Emerging trends in communications and social science. Biodiversity Project. Source: https://www.comminit.com/en/node/223510/306.

Forcht KA, Pierson JK, Bauman BM (1988). Developing awareness of computer ethics. Proceedings of the ACM SIGCPR conference on

Management of Information Systems Personnel. Maryland USA, pp. 142-143.

Fishbein M, Ajzen I (1975). Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. Reading, MA: Addison-Wesley.

Hagen JM, Albrechtsen E, Hovden J (2008). Implementation and effectiveness of organizational information security measures. Information Manage. Comput. Secur., 16(4):377-397.

Hubbard W (2003). Methods and techniques of implementing a security awareness program. Sans Infosec Reading Room-Security Awareness. Source: http://www.sans.org/reading_room/whitepapers/awareness/methods-techniques-implementing-security-awareness-program_417.

Information security forum (2003). The standard of good practice for information security. Source: http://www.netbotz.com/library/Info_Security_Forum_Standard_Good_Practices.pdf.

Kruger HA, Kearney WD (2006). A prototype for assessing information security awareness. J. Comput. Secur.. 25(4): 289-296.

Levin M, Klev R (2002). *Forandring som praksis : læring og utvikling i organisasjoner*. In Norwegian [Changes in practice: learning and development in organizations] Bergen, Fagbokforlaget.

Newbould M, Furnell S (2009). Playing Safe: A prototype game for raising awareness of social engineering. Proceedings of the 7th Australian Information Security Management Conference. pp. 24-30.

Namjoo C, Dan K, Jahyun G, Andy W (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. Inform. Manage. Comput. Secur., 16(5):484–501.

O'Connor TJ, Fitzgerald SG, Cooper RA, Thorman TA, Boninger ML (2001). Does computer game play aid in motivation of exercise and increase metabolic activity during wheelchair ergometry? Med. Eng. Phys., 23(4): 267–273.

Swanson M, Bartol N, Sabato J, Hash J, Graffo L (2003). Security metrics guide for information technology systems. NIST special publication 800-55.Source:http://webharvest.gov/peth04/20041027033844/http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf].

Wilson M, Hash J (2003). Building an Information Technology Security Awareness and Training Program. NIST special publication 800-50. source: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

Triangle Air Awareness, source: http://triangleairawareness.org/?p=55.

Blast N Quit, source: http://captaind-pc-gaming.blogspot.com/2010/01/quit-smoking-with-help-of-video-games.html.