2008

IT Security Expert's Presentation and Attitude Changes of End-Users Towards IT Security Aware Behaviour: A Pilot Study

Md Mahbubur Rahim
Clayton School of Information Technology Monash University Australia, mahbubur.rahim@infotech.monash.edu.au

Ai Cheo
Clayton School of Information Technology Monash University Australia

Kevin Cheong
Clayton School of Information Technology Monash University Australia

IT Security Expert's Presentation and Attitude Changes of End-Users Towards IT Security Aware Behaviour: A Pilot Study

Md Mahbubur Rahim
Ai Cheo
Kevin Cheong
Clayton School of Information Technology
Monash University
Australia
Email: mahbubur.rahim@infotech.monash.edu.au

Abstract

IT security expert's presentation is one of the most advocated strategies to improve end-users' information security aware behaviour. However, no systematic evaluation has yet been reported in the IT literature to comprehensively evaluate the effectiveness of this strategy. To address this gap, a theory driven instrument was developed to evaluate the effectiveness of IT security expert's presentation for enhancing the attitudes of end-users towards engaging in information security aware behaviour. The findings, which confirm a positive influence of IT security expert's presentation strategy, can be used to evaluate the effectiveness of other educational strategies.

Keywords

IT security, attitudes, end-users, IT expert's presentation, pilot study

INTRODUCTION

Rapid advancement taking place in Information and Communication Technologies (ICT) has greatly improved the ease with which end-users gain access to critical corporate information (Hansford 2006). This however presents a challenge for organisations from the security perspective as the integrity of information can be easily compromised. Hence, there is a need for developing staff appreciation to support security mechanisms that organisations want to introduce for safeguarding their information and IT assets. According to Kruger and Kearney (2006), sustaining security aware behavior is crucial for an effective information security environment. This is because the lack of demonstrating appropriate information security aware behavior by end-users may result in significant organisational losses. The successful operation of an organisation thus largely depends on all employees exhibiting information security aware behavior. This is however not an easy task as a recent AusCERT survey discovered that the most challenging aspect of security management is changing users' attitudes and behavior concerning computer security practices (AustCERT 2006).

In order to help improve end-users' information security behavior, several educational strategies (e.g. discussion sessions, lab sessions, videos, simulation, workshops, and presentations by IT experts) are proposed in the IT literature. However, the attractiveness of these strategies is low because they have not been evaluated rigorously using empirical evidence. This initial pilot study was thus undertaken to address the abovementioned gap in the IT security literature. This is done by developing a theory-driven instrument and administering it at two points in time with a group of student-users to evaluate the effectiveness of using an IT security expert's presentation as a strategy to raise end-users' attitude towards information security aware behavior. According to Peltier (2005), presentation by an IT speaker involves giving an oral talk using audio-visual tools which are directed at organisational end-users and discussing the key aspects of information security.

The pilot study findings confirm a positive influence of IT security expert's presentation strategy on attitudes changes of end-users. This observation is useful because it helps in increasing confidence of IT managers in using an IT expert's presentation strategy to improve employees' information security aware behaviour due to a strong correlation that exists between attitudes and actual behaviour of individuals. As for knowledge, the instrument forms an empirical foundation which can be used in evaluating the effectiveness of other kinds of educational strategies. The instrument also serves as a template for IT security researchers who may like to extend it to measure attitudes towards security aware behavior of end-users with regard to a specific type of IT applications (e.g. mobile commerce).

The rest of the paper has been organised as follows. First, a literature analysis of the strategies used in promoting end-users' security aware behaviour and key areas comprising information security aware behaviour is provided. Then, the research approach is described. Next, the development and validation of an instrument

based on the relevant theories is discussed. The results of the pilot study are then presented and discussed. Finally, the importance of the findings, limitations of the research and future directions of research are highlighted in the conclusion section.

LITERATURE ANALYSIS

The existing literature on information security aware behaviour is analysed from two distinct perspectives: strategies used for promoting end-users' security aware behaviour and key areas comprising information security aware behaviour. Each perspective is explained below.

Strategies Used for Promoting End-Users' Security Aware Behaviour

A rich body of literature exists that focuses on the strategies used for promoting end-users' security aware behaviour. This literature can be divided into three broad streams. The first stream merely acknowledges the need for end-users' security aware behavior, but does not explain any particular strategy in details. Typical studies representing this stream include the works of Siponen (2001) and Schultz (2004). In his study, Siponen (2001) explains the reasons for demonstrating information security aware behaviour and highlights five dimensions of information security aware behaviour. In another study, Schultz (2004) discusses why security training and awareness currently has low priority in organisations. The second stream suggests strategies to increase information security aware behavior. Two types of strategies are identified: traditional guidelines and frameworks and unconventional approaches. Guidelines imply general tips and suggestions. For example, Bresz (2004) offered several guidelines for increasing awareness on such topics as security reminders, protection from malicious software, and password management. In another study, Wood (1995) listed 50 awareness raising efforts which cover everything from conducting risk assessments, automated questionnaires, to security reminders on coffee mugs. On the other hand, frameworks represent a more formal structured approach where suggestions appear in some order. For example, an awareness raising framework based on several motivation and behavioral theories was the basis of Siponen's (2000) work. Valentine (2006) recommended a three phased methodology to create security awareness of users. Typical unconventional approaches include the works of Spurling's (1995) and Sommers and Robinson (2004). A case study is the basis of Spurling's (1995) work which features an Australian company that experienced many user related security problems which were resolved through a multitude of strategies including newsletters, books, and staff training. In another study, Sommers and Robinson (2004) discussed filming three short, funny videos that demonstrated the serious messages of information security aware behavior in their work. The third stream of literature includes studies which focus on developing tools to measure end users general awareness on information security. The study of Kruger and Kearney (2006) represents a typical example of this line of research. In their study, Kruger and Kearney (2006) developed a prototype model that aimed to ensure that computer users are aware of the risks associated with using IT, and understand and obey policies and procedures in place. A questionnaire was created, weighted, and refined, and sent out to employees of a mining company. The results from the questionnaire were used to evaluate the effectiveness of the prototype.

It is interesting to note that several studies (Peltier 2005; Spurling 1995) representing the second stream acknowledge the value of an IT security expert's presentation as an effective means to enhance end users' information security aware behavior. However, none has offered a theory driven systematic evaluation of the effectiveness of this strategy. Although the third stream made an attempt to measure security awareness it did not measure the effectiveness of any particular educational strategy. To address this gap in the literature, this project thus makes an attempt to evaluate the effectiveness of IT security expert presentations in raising end-users' propensity to engage in information security aware behaviour. It is however argued that direct observations of end-users' information security aware behavior are difficult. Hence, a proxy to security aware behavior needs to be identified. End-users' attitude toward information security aware behavior is considered to be a substitute to their intended behavior because of the close relationship between these variables. Therefore, the well known Theory of Planned Behavior (Ajzen 1991) selected from the social psychology literature is chosen as the reference framework to evaluate the effectiveness of IT security expert's presentation as a strategy to raise attitude of end-users to demonstrate information security aware behaviour.

Key Areas Comprising Information Security Aware Behaviour

A total of five broad areas of information security aware behaviour are identified. Each area is described below:

Password Management

Password security is essential to the security of information systems (Gehringer 2002). While the majority of organisational and home users rely heavily on user-generated passwords as a basic form of authentication to sensitive information and personal resources, the insecure creation of passwords and password usage could open the first door to a malicious attacker. In contrast, good password management behaviour can be a defense against intrusion into a computer system (Microsoft 2006; Monash University 2006a; Monash University

2006b). In their study, Zviran and Haga (1999) investigated the core characteristics of user-generated passwords and associations among those characteristics. Their findings confirm that user-selected passwords are still being made up of the characteristics of personal details meaningful to the user, are relatively short, are comprised of alphanumeric characters, are rarely changed, and are usually written down. These findings indicated a need to raise the security consciousness of system users. Many organisations and practitioners provide guidelines on good password security practices which if adopted can help protect information resources from both external and internal attacks.

Email Management

Another vital component of information security aware behaviour is email management. A key aspect of email management is concerned with spam emails. Spam email is unsolicited email that may consist of commercial advertising, pornography or get-rich-quick schemes (Monash University 2006b). The problems posed by spam have grown from simple annoyances to security issues such as virus attacks. The deluge of spam costs up to an estimated $20 billion each year in lost productivity (Lyman 2003). Users can help limit the chances of being attacked by being security cautious and taking actions against spammers and by following a good email management practice (CERT 2002; O' Reilly 2005; University of California 2006).

Workstation Security

The term "workstation" is often used in a broad sense in which it refers to any electronic device (e.g. laptop, desktop PC, PDA) used for information storage and processing. Security risks associated with workstations are great. According to the University of Miami (2008), workstation security should be addressed as part of physical safeguards and end-users should be educated about the need for having such safeguards. Existing security literature identifies several common security risks to the integrity and information content stored within today's workstations. The size of the standard and smaller notebook PCs, which are often used as portable workstations at work, home or whilst traveling, makes them particularly vulnerable to theft (Eracom Technology 2008). According to the IT gurus, workstation security should involve many well-publicised guidelines including keeping sensitive data backup in locked drawers, using encryption techniques for emails, backing up important files, logging off or turning off workstations after use among others.

Malicious Software Protection

Malicious software, commonly known as 'malware" is a software inserted into an information system to cause harm to that system or other systems, or to subvert them for uses other than those intended by their owners (OECD Report 2008). Malware affects everyone: government, business and individual users. However, it is the individual home users who are more vulnerable because of their lack of awareness about the possible harmful effect of malware. Different types of malware are commonly observed including virus, worms, spyware among others. As the reliance of home users on the Internet increases so do the threat of malware. The lack of user awareness and their subsequent inaction contributes to the increasing prevalence of malware. The number of new viruses discovered every month continues to increase (CAIDA 2006). The Global Information Security Survey 2005 (CSI 2005) found that virus attacks are the source of the greatest financial losses. Without any protection against viruses, users could become the unwitting vehicle for disrupting the information systems in the organisation. Good malware protection practices consist of installation of anti-virus software, keeping anti-virus software updated, use of firewall and installation of software patches among others.

Internet Browser Security

An Internet browser is the window of a user to the World Wide Web. The better and safer is the browser, the more a user will see and experience. To enhance one's Internet experience, most modern Internet browsers shield against all types of viruses (TopTenREVIEWS 2008). However, the browser itself has become a source of security concern because according to a recent PCWorld report (Spanbauer 2007), internet browsers have become a popular target for internet attacks. As a result, it is necessary for the end-users to remain aware of the need to continuously install security patches and upgrades. Many IT gurus advocate the use of an internet browser which has a phishing filter and keeping that filter constantly enabled.

RESEARCH APPROACH

A three-stage research design was followed. Stage 1 is concerned with identifying core areas relevant to information security aware behaviour and generating a set of items to operationalise those areas. Stage 2 is about validating the preliminary instrument developed based on the items generated in the previous stage. This is done through the use of a focus group and a qualitative pre-test study. The focus group comprises 3 IT security experts and 2 academics whose areas of research include IT security. The feedback received from these focus group members were analysed in terms of relevance, completeness, and duplication of areas, items and the overall format of the questionnaire. On the other hand, the participants of the pre-test involve 4 postgraduate IT students who have prior job experience. These students were required to perform two tasks: firstly, they were to

indicate how appropriate each security area was to addressing information security aware behavior; and secondly, they were to match each individual item to its appropriate security area and then indicate how well the item represents that particular area. Stage 3 concerns with conducting a pilot study which involves the administration of the revised questionnaire which was distributed among 25 students (both under-graduate and post-graduate). They were selected by placing an advertisement in a university portal. Each student was given an incentive of A$20 for his/her involvement in the pilot study. They were asked to complete the revised questionnaire, listen to an IT security expert's presentation, and then complete the same instrument again.

Prior to the commencement of the IT speaker's presentation, the researchers addressed the participating students clarifying the purpose of the research and adopted the following strategies in order to minimise the social desirability bias of the participating students: a) the students were advised that the financial incentive (i.e. A$20) given to them would not be related to the level of their attitudes, b) the students were not required to write any information on their instrument that could possibly lead the researchers to identify them and thus there was no opportunity for the researchers to probe students to further clarify their attitudes formation after attending the IT speaker's presentation, and hence students could safely report their attitudes without trying to satisfy the expectations of the researchers, and c) students were advised to indicate their candid and honest views rather than to inflate their views due to the incentives offered to them.

In addition, to address the effect of any treatment bias, the following strategies were followed by the researchers: a) the participating students were not allowed to interact with the speaker during the presentation to avoid any influence that may arise as a result of speaker's personality, charisma or appearance, b) the speaker was advised to create a friendly and flexible atmosphere (using such techniques as jokes) and deliver presentation in simple English (rather than using technical jargons) so that students could treat the speaker as a security expert rather than an imposing authoritarian figure and as such the actual job title of the speaker was not mentioned, and c) students were advised to ignore the influence of gender of the speaker (i.e. the fact that speaker was a male person does not translate into greater security related knowledge than that of a female speaker). In other words, students were given clear instructions for not considering such issues as gender, charisma and delivery style of the speaker as important moderating factors for reporting their honest views on attitudes towards information security aware behaviour.

The data collected from the pilot study were analysed using SPSS (a well-known statistical package). Using this package, a set of parametric and non-parametric test was performed. Details for selecting these tests are described in the results section.

INSTRUMENT DEVELOPMENT & VALIDATION

Based on a review of the related literature, five broad areas comprising information security behaviour were identified. These are reported in the second part of the literature analysis section. The broad areas include: password management (Bresz 2004; Cox et al. 2001; Uday 2005), email management (Cox et al. 2001; Johnson 2006), workstation security (Cox et al. 2001; Johnson 2006; Peltier 2005; Uday 2005), malicious software protection (Smith 2005; Sommers and Robinson 2004) and internet browser security (Cox et al. 2001; Smith 2005). A total of 38 items were also prepared to operationalise these five areas. Out of these, 12 items were used for password management, 4 items for email management, 8 items for workstation security, 9 items for malicious software protection and 5 items for internet browser security. Furthermore, out of 38 items, 17 items have negative endpoints because mixing positive and negative endpoints helps prevent participants from responding to items in the same way regardless of content (Francis et al. 2004). A six-page long preliminary instrument was finally developed and participants were required to respond to each item on a 7-point scale where 1 means least important, 4 means neutral and 7 stands for most important. A 7-point scale was chosen because it helps minimize a ceiling effect (Zimet et al. 1988).

The preliminary instrument was then distributed among the focus group members for their critical evaluation of the items. A total of 17 suggestions were received from these members. Their feedback falls into the following aspects: adding new items/areas, removing existing items/areas, rewording existing items/areas, grammatical changes in items/areas, and changes in some aspects of the questionnaire format. All members of the focus group agreed that the five areas (i.e. password management, email management, workstation security, malicious software protection and internet browser security) adequately address all the key aspects of information security aware behavior. Hence, there was no need to include any additional areas. Out of 19 suggestions, 15 were regarding rephrasing existing items, 2 were about the removal of two existing items that had somewhat overlapping meanings, and the remaining 2 were concerned with the overall format of the questionnaire. After a careful review of these suggestions, necessary rewording of the 15 items were incorporated to improve clarity, 1 item was removed to avoid redundant meanings, and changes in the format were made to enhance the presentation of the questionnaire.

In the first part of the pre-test, 4 postgraduate students were requested to indicate the degree of importance of each security area on a scale of 1 to 5 (where 1 represents 'extremely unimportant' and 5 represents 'extremely important'). The responses of the students are shown in Table 1. The mean ratings of these students for each area are: password management (5), email management (4), workstation security (4.25), malicious software protection (4.25) and internet browser security. The mean data thus indicates that all the areas were at least 'somewhat important'. Hence, none of the areas were excluded from the instrument.

Table 1: Degree of importance of instrument areas

	Areas				
Participants	Password Management	Email Management	Workstation Security	Malicious Software Protection	Internet Browser Security
A	5	4	4	4	3
B	5	5	4	4	5
C	5	4	5	4	4
D	5	3	4	5	4
Mean rating	5	4	4.25	4.25	4

In the second part, these students were given a list of all the items in the instrument in a random order. They were asked to match each item to its appropriate area. The following guideline was used: an item would be revised when it is not assigned to the same type of security area by at least three of the participants. For example, item 7 (which is 'Passwords that are of reasonable length are effective') was assigned to 'password management' area by students A, C, and D, but was assigned to 'email management' area by student D. This means that three out of four students associated this item with its correct security area. However, if student A related item 7 with 'internet browser security', it would imply that this item is not clearly stated and would need to be improved. The responses from the students participating in the pre-test indicate that all items received either three out of four, or total agreement among students. Therefore, the clarity of the instrument is reinforced and no items were rephrased or deleted.

Next, these students were asked to rate how well each matched item represents the area which it is intended to represent. Their responses are shown in Table 2. The rating was achieved on a scale of 1 to 5 (where 1 represents 'not at all' and 5 represents 'very well'). A mean rating of less than three would indicate that the item represents very little of an area and hence it needs to be discarded. A mean rating of three or greater, would be an indicator of good quality design as the choice of item was not ambiguous, as well as relevant to information security aware behavior. Based on the student responses, only one item was removed as it received a mean rating of 2.25. The revised instrument is then administered among a student sample to evaluate the effectiveness of an IT security expert's presentation.

RESULTS

Out of 25 students who took part in Stage 3 (discussed earlier), 9 are female and the remaining 16 are male. Their mean age is less than 30 years. The overall attitude of students towards information security aware behaviour prior to conducting IT security expert's presentation was measured and is summarised in Table 3. This table also indicates the aggregate means of student responses for each of the five security area. As there are now 36 items to measure a student's overall attitude and each item varies on a scale of 1 to 7, the aggregate mean attitude of an individual could vary between 36 and 252 (i.e. 36x7). A close look at Table 3 indicates that the aggregate mean attitude of the student group is 204.64. This implies that the participating students in general have a favourable attitude towards the need to demonstrate information security aware behaviour because the value of the aggregate mean attitude lies far above the neutral value of 144 (36x4) on the attitude scale.

Table 2: Degree of importance of instrument areas

No	Item description	Mean Rating	No	Item description	Mean Rating
1	Writing down passwords is a good practice	5	20	Regularly changing passwords is useful	4.75

2	Having anti spyware software installed is of little use	4	21	Refraining from downloading files from unfamiliar or untrustworthy websites is essential	4.00
3	Running a complete system scan for viruses every 2 or 3 weeks is a waste of time	3.5	22	Memorizing passwords is imperative	4.75
4	Checking email attachments for viruses before opening them is a waste of time	3.75	23	Abiding by workstation policies and rules (downloading restrictions, appropriate websites) is not important	2.25
5	Maintaining different passwords for different online accounts (e.g. email, banking, eBay etc.) is a good practice	4.75	24	Having an internet browser which has a phishing filter is important	4.50
6	Reporting incidents to the appropriate technical staff is not advisable	3.75	25	Using words such as family members, or pets' names as passwords is safe	4.50
7	Passwords that are of reasonable length (8 or more characters) are effective	4.75	26	Keeping the table and workstation area clear of important or confidential notes, memos and other documents is essential	3.00
8	Using encryption techniques for emails (or other forms of messages) with highly sensitive or confidential information is vital	4.75	27	Sharing passwords with close friends is a good practice	3.00
9	Logging off or turning off the computer after use is imperative	4.25	28	Using an email service's spam filter is valuable	4.75
10	Having a virus protection program (e.g. McAfee, Norton) installed is unsafe	3.75	29	Having a firewall installed is a safe practice	4.00
11	Leaving the workstation unattended is safe	4.50	30	Updating antivirus software is important	4.50
12	Keeping anti spyware software constantly enabled is not important	4.50	31	Passwords that are easy to remember are useful	3.75
13	Keeping sensitive data backup in locked drawers, desks and cabinets is not important	3.00	32	A virus protection program that is constantly enabled is essential	4.50
14	Knowing the sender of the email (person or company) before opening it is important	4.50	33	Securing all recording media (flash disks, portable hard drives, compact disks etc.) after leaving the workstation is important	4.75
15	Sharing passwords with anyone is safe	4.75	34	Passwords that consist of both letters and numbers are more effective than passwords with only letters	5.00
16	Backing up important files (on a CD, DVD, portable hard drive or flash drive) once every few days is not important	3.00	35	Keeping an internet browser's phishing filter constantly enabled is of little use	3.75
17	Using common terms such as dictionary words as passwords is unsafe	5.00	36	Passwords that last longer than 2 or 3 months are useful	3.75
18	Keeping firewalls constantly enabled is essential	4.50	37	Providing personal details to any kind of online advertising is appropriate	3.75
19	Giving out personal details including credit card numbers only to trustworthy websites is appropriate	4.50			

Looking at the fifth column of Table 3, it can be suggested that student attitudes towards email management are more favorable than those of workstation security, password management, malicious software security and internet browser security. This is because the ratio of student attitude as compared to maximum possible attitude with regard to e-mail management (i.e. 85%) is greater than those of malicious software security (78%), internet browser security (78.32%), password management (78.3%), and workstation security (80%). Immediately after

the completion of the IT expert's presentation, the same instrument was distributed among the same student group and their responses were analysed. The aggregate mean of the student's attitude towards each security area and the overall attitude towards information security aware behaviour after the IT expert's presentation are shown in the fourth column of Table 3. It can be noted that the aggregate mean attitude of the student group is now 223.76. This implies that overall the participating students' attitudes have increased (from 204.64 to 223.76). Table 3 further indicates that the aggregate mean of student attitude towards each of the five areas have increased after the speaker's presentation. Again the last column of Table 3, suggests that in the posttest, attitudes towards e-mail management and malicious software protection became more favorable than password management, internet browser security, email management, and workstation security. The trend of greater awareness about e-mail management has not been changed.

Table 3: Student attitudes towards information security aware behaviour

Security Areas	Maximum Possible Attitude	Actual Student Attitude (Aggregate Means)		Ratio of Actual Student Attitude to the Maximum Possible Attitude	
		Pre-Presentation	Post-Presentation	Pre-Presentation	Post-Presentation
Password management	84	65.80	73.04	78.3	86.9
Email management	28	23.92	25.56	85.4	91.2
Workstation security	49	39.24	43.40	80.0	88.5
Malicious software security	56	48.36	52.40	78.0	93.5
Internet browser security	35	27.32	29.36	78.32	83.8
Overall attitude	252	204.64	223.76	81.2	88.7

Before performing suitable statistical tests to determine whether significant differences exist between student attitudes prior and after the IT expert's presentation, it is important to verify whether the attitude data follows a normal distribution. This was achieved using the Shapiro-Wilk normality test for both pretest and posttest attitude data. The Shapiro-Wilk values for pre and post-presentation attitude responses are: 0.805 and 0.159. As these values are greater than 0.05, the distribution of student responses can be assumed to follow a normal distribution. In order to find out whether there exists a statistically significant difference in the overall attitude of students prior and after the expert's presentation, a paired-sample t-test (2-tailed) was conducted with a 95% confidence interval. The results of the paired-sample t-test (shown in Table 4) indicate the existence of a significant difference in student attitudes confirming the existence of a very strong effect of the speaker's presentation in raising student attitudes towards information security aware behaviour.

Table 4: Results of Paired-Samples t-test

	Paired Differences						
	95% of the Confidence Interval of the Difference						
Security Areas	Mean	Standard Deviation	Standard Error Mean	Lower	Upper	t	p-value
Password management	-7.24	6.66	1.33	-9.99	-4.49	-5.44	.000
Email management	-1.64	3.34	.67	-3.02	-.26	-2.46	.022
Workstation security	-4.16	4.87	.97	-6.17	-2.15	-4.27	.000
Malicious software protection	-4.04	4.30	.86	-5.81	-2.27	-4.70	.000
Internet browser security	-2.04	4.19	.84	-3.77	-.31	-2.43	.023
Overall attitude	-19.12	11.53	2.31	-23.9	-14.36	-8.29	.000

However, due to small size of the sample, the Wilcoxon test (a non-parametric test) was also performed to determine if the difference in the overall attitude of students prior and after the expert's presentation is statistically significant. This test was chosen because it is alternative to the student's t-test. The merit of using the Wilcoxon test is that it does not require assumptions about the normal distribution form of attitude data (Wilcoxon, 1945) . The results of the Wilcoxon test (shown in Table 5) are consistent with the broad findings of the paired student t-test; thus providing further support to the assertion that IT speaker's presentation had a significant impact in improving students' attitudes towards information security aware behaviour. The Wilcoxon test results further indicate that student attitudes towards each of the five security areas have significantly improved as well.

Table 5: Results of Wilcoxon test

Security Areas	Mean Negative Ranks	Mean Positive Ranks	z	p-value
Password management	10.00	13.95	-2.76	.006
Email management	7.00	11.07	-2.42	.015
Workstation security	10.73	9.80	-2.10	.036
Malicious software protection	10.44	13.38	-2.16	.030
Internet browser security	9.46	14.77	-.749	.045
Overall attitude	10.14	15.25	-1.37	.017

DISCUSSION

As the results of post-test attitude scores are considerably higher than those prior to the IT expert's presentation, it can be argued that students are more likely to engage in an increased level of information security aware behaviour because of the theoretically predicted strong relationship that exists between a person's attitude towards a behaviour and actual execution of the behaviour by that person. Significant differences in student attitudes are also observed in relation to each of the five security areas. This is evident from the p-values of both student t-test and Wilcoxon test as indicated in the last column of Tables 4 and 5. Therefore, IT expert's presentation is effective in changing end-users' attitude in all these five areas.

However, of all the five areas, attitudes towards password management and malicious software protection were more affected than those of internet browser security, email management and workstation security. This observation is confirmed by the p-values shown in Tables 4 and 5. In other words, internet browser security and email management were less sensitive to changes in attitude in the posttest. This can be explained in two ways: first, the participating students may already have a greater familiarity with those areas; second, it may be possible that the speaker did not discuss internet browser security and email management aspects in greater details.

Drawing on the findings, it can be reported that although IT speaker's presentation was found to have a significant impact in changing student attitudes towards information security aware behaviour but it is not possible to claim that such a change in student attitudes would last for a long period of time. In other words, the short term effect of IT speaker's presentation on students' attitude changes was supported but the long term effect cannot be assumed from the pilot study.

CONCLUSION

In today's digital environment, maintaining a positive attitude of end-users towards information security aware behaviour is important to safeguard critical organisational IT resources. IT security expert's presentation is one of the most advocated strategy to raise end-users' information security aware behaviour. However, no systematic evaluation has yet been reported in the IT literature to comprehensively evaluate the effectiveness of this strategy. To address this gap, this paper reports an empirical evaluation of the effectiveness of IT security expert's presentation to enhance end-user's attitudes towards information security aware behaviour. This is achieved by developing a theory driven instrument for operationalising the attitude of end-users towards information security aware behavior. As this is a theory driven instrument, its use in evaluating the effectiveness of an IT speaker's presentation as a strategy to raise users' attitude towards information security aware behavior is more acceptable than relying on anecdotal evidence from users. The finding of this study is thus significant to IT researchers because the instrument would enable the establishment of statistical generalisability of using an IT security expert's presentation as an effective strategy for raising attitude towards information security aware behavior. The finding is also important to IT practitioners for it forms an empirical foundation which can be used in evaluating the effectiveness of other strategies.

There are some notable limitations of this study that need to be reported. Firstly, a group of postgraduate students with some job experience were invited to participate in the pilot study. In a real life setting, IT managers are likely to have far greater experience than those students. Therefore, the feedback received from the students may not demonstrate the maturity of IT managers. As a result, an opportunity for identifying some new items describing concerns for information security may have been lost. Secondly, due to the small size of the sample, the results should be treated with caution. Thirdly, there was a lack of adequate attention paid to address the treatment effect in the experiment. More specifically, issues like the influence of gender, charisma, appearance, and degree of expertise in IT security area demonstrated by the speaker were not scientifically controlled although an attempt was made by the researchers to make participating students aware of these factors on the formation of their attitudes.

This study thus can be extended in several ways: a) this study would have benefited from a large sample with organisational end-users as opposed to a student sample, b) the instrument should be tested by managerial end-users who may have different views from student users, and c) the IT security expert presentation could have been altered in a number of ways like changing the speaker, lengthening the duration of the presentation, or changing the type of presentation (e.g. assisted with a story or audio/visual clips) to find out whether such variations can influence the results, d) It would be interesting to invite someone who is not an IT speaker deliver the same presentation to the similar types of student sample and measure their attitude improvement. This would help in identifying possible intervening effect of the IT speaker's characteristics.

REFERENCES

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes*, (50:2), December, pp 179 – 211.

AustCERT 2006. "Computer Crime and Security Survey 2006." Retrieved 14 September, 2006, from http://www.auscert.org.au/images/ACCSS2006.pdf

Bresz, F.P. 2004. "People – Often the Weakest Link in Security, But One of The Best Places to Start," *Journal of Health Care Compliance*, (4:1), pp 57 – 60.

CAIDA 2006. "CAIDA Analysis of Code-Red." Retrieved 25 October, 2006, from http://www.caida.org/analysis/security/code-red/

CERT 2002. "Email Bombing and Spamming." Retrieved 6 November, 2006, from http://www.cert.org/tech_tips/email_bombing_spamming.html

Cox, A., Connolly, S., and Currall, J. 2001. "Raising Information Security Awareness in the Academic Setting." *Vine* (123:11), pp 11 – 16.

CSI 2005. "2005 CSI/FBI Computer Crime and Security Survey." Retrieved 3 December, 2006 from http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf

Eracom Technology 2008. White Paper on Workstation Security.

Francis, J., Eccles, M., Johnston, M., Walker, A., Grimshaw, J., Foy, R., Kaner, E., Smith, L., & Bonnetti, D. (2004) Constructing questionnaires based on the theory of planned behaviour: A manual for health services researchers, center of Health Services Research, United Kingdom.

Gehringer, E.F. 2002. "Choosing Passwords: Security and Human Factors", *International Symposium on Technology and Society, ISTAS'02,* pp 369-373

Hansford, P. 2006. "Make your people aware." Retrieved 9 August, 2006, from http://www.scmagazine.com/uk/news/article/563841/make-people-aware/

Johnson, E.C. 2006. "Security Awareness: Switch to a Better Programme," *Network Security* (2), pp 15 – 18.

Kruger, H.A., Kearney, W.D. 2006. "A Prototype for Assessing Information Security Awareness," *Computers and Security* (25), pp 289 – 296.

Lyman J. 2003. "Spam Costs $20 Billion Each Year in Lost Productivity", Retrieved 3 November, 2006 from http://www.linuxinsider.com/story/32478.html

Monash University 2006a. "Unwanted/Unsolicited Email or Spam." Retrieved 25 August, 2006 from http://www.its.monash.edu.au/staff/email/spam/

Monash University 2006b. "Beware of Malicious Emails and Web Pages." Retrieved 25 August, 2006 from http://www.its.monash.edu.au/staff/security/staff-only/home/emails.html

Microsoft 2006. "Strong Passwords: How to Create and Use Them." Retrieved 29 August, 2006 from http://www.microsoft.com/athome/security/privacy/password.mspx

OECD Report 2008. "Malicious Software (Malware): A security threat to the internet economy", *Ministerial Background Report,* Seoul, Korea, 17-18 June.

O' Reilly, D. 2005. "10-step Security." Retrieved 29 August, 2006 from http://www.pcworld.com/article/id,122500-page,1/article.html

Peltier, T.R. 2005. "Implementing an Information Security Awareness Program," *Information Systems Security*, (14: 2), pp. 37.

Schultz, E. 2004. "Security Training and Awareness – Fitting a Square Peg in a Round Hole," *Computers and Security*, (23), pp 1 – 2.

Siponen, M.T. 2000. "A Conceptual Foundation for Organizational Information Security Swareness," *Information Management & Computer Security*, (8:1), pp 31 – 41.

Siponen, M.T. 2001. "Five Dimensions of Information Security Swareness," *Computers and Society* (8:1), pp 24 – 29.

Smith, R.F. 2005. "Security Awareness – Win Users Over to Your Company Policy," *Windows IT Security*, (5:12), pp 10.

Sommers, K., and Robinson, B. 2004. "Security Awareness Training for Students at Virginia Commonwealth University." *Proceedings of SIGUCCS.*. Baltimore, MD, USA.

Spanbauer, S. 2007. "Thwart the Three Biggest Internet Threats of 2007", *PCWorld*, January 24.

Spurling, P. 1995. "Promoting Security Awareness and Commitment." *Information Management & Computer Security*, (3:2), pp 20 – 25.

TopTenREVIEWS 2008. "Internet Browser Software Reviews 2008." Retrieved 12 June, 2008 from http://internet-browser-review.toptenreviews.com

Uday O, A.P. 2005. "Awareness Training: Strengthening Your Weakest Link," *Certification Magazine*, (7:8), pp 28 - 29.

University of California 2006. "Email Safety Tips." Retrieved 11 June, 2008 from http://www.security.uci.edu/email/

University of Miami 2008. "Data Protection Report." Retrieved 10 June 2008 from http://privacy.med.miami.edu/glossary/xd_workstation_security.htm

Valentine, J.A. 2006. "Enhancing the Employee Security Awareness Model," *Computer Fraud & Security*, (6), pp 17 – 19.

Wikipedia 2006. Security awareness. Retrieved August 31, 2006 from http://en.wikipedia.org/wiki/Security_awareness (not cited in body, delete?)

Wilcoxon, F. (1945). Individual comparisons by ranking methods. *Biometrics, 1*, 80-83.

Wood, C.C. 1995. "Information Security Awareness Raising Methods," *Computer Fraud & Security Bulletin*, (5), pp 13 – 15.

Zimet, D., Dahlem, N.W., Zimet, S.G., and Farley, G.K. 1988. "The Multidimensional Scale of Perceived Social Support," *Journal of Personality Assessment*, (52:1), pp 30-41.

Zviran, M., and Haga, W.J. 1999. "Password Security: An Empirical Study," *Journal of Management Information Systems*, (15:4), pp 161-185.

COPYRIGHT