A Cross-Cultural Investigation Of Situational Information Security Awareness Programs

Authors:
Charlie C. Chen, B. Dawn Medlin, R.S. Shaw

Abstract

Purpose – The aim of this research is to make users aware of the importance surrounding the issue of security and security awareness while at the same time making educators as well as other individuals aware of the differing effects of cultural dimensions into the learning process.

Design/methodology/approach – An inter-cultural study was conducted to investigate if users from the USA and Taiwan exposed to the same situational awareness learning would have different performance in those security awareness outcomes.

Findings – The findings confirm that American users who received the situational learning outperformed those users who received the traditional face-to-face instruction. Taiwanese users did not perform significantly differently between these two treatments.

Research limitations/implications – The study was only focused on two countries and therefore may limit its implications worldwide. But the study does show that global citizens also react differently to security awareness as would be expected due to differing cultures. Certainly, awareness of the risks and safeguards is the first line of defense that can be employed by any individual, but how individuals address these risks can be very dissimilar in different cultures. Therefore, the implications are apparent that the issue of security awareness should be studied from different cultural perspectives.

Originality/value – This paper offers original findings and value into the investigation of whether or not situational security awareness training is culturally-bounded

Charlie C. Chen, B. Dawn Medlin, R.S. Shaw (2008) "A Cross-Cultural Investigation Of Situational Information Security Awareness Programs" *Information Management & Computer Security* vol. 16(4) pp. 360-376 Version Of Record Available At www.emeraldinsight.com

A Cross-Cultural Investigation Of Situational Information Security Awareness Programs

1. Introduction

Security awareness training of general users is negligible in many developing and under-developed countries. Additionally, the diffusion of the Internet and prevalent social technologies in both of these aforementioned types of countries impose grave threats to information security.

Security awareness involves the human factor. No matter how advanced and stringent the security technological solutions, humans are generally the first line of defense to secure information assets. Security breaches, such as virus infections, identity theft, and dumpster diving, are the direct cause of carelessness and a lack of knowledge and action on the part of users. Technological solutions are effective only after users are knowledgeable and skillful at using them. Therefore, security

awareness can be more important than the technology factor in contributing to the success of today's information security.

Thus, cultivating security awareness in relation to an individual, a corporate, and on a global basis is a prerequisite to a more secure and protected world within the realm of information. A 2006 information security breaches survey found that the gap between the companies that have high security awareness and those that did not is widening (PriceWaterHouseCoopers, 2006). This gap may be explained in the fact that the larger enterprises spend more time in developing security policies, training, and institute proactively security measures such as anti-virus software. In the same logic, one effective approach to better secure a person's information is to make individuals as well as organizations more aware of security risks and their responsibilities.

In general, security awareness programs provide users adequate knowledge to evaluate adverse consequences of security problems and take the appropriate actions to prevent and correct security breaches. International firms, such as DaimlerChrysler (Grant, 2007), consider security awareness of their employees as one of key performance indicators to their successful operation. Members of the European Network and Information Security Agency, representing 67 government departments and private companies in nine European countries are actively conducting internal and external auditing to assess their actual state of security awareness (Filipek, 2007). Although different countries may have different states of security awareness, the increase of security awareness of their national, corporate and citizen safety is unequivocally important for all countries. It is imperative that general users of all cultural backgrounds receive proper security awareness training in order to reduce security risks to themselves and to others.

Different parts of the world have varying technological capacities and security challenges. Though this may be the case, improving the level of security awareness of general users is equally important in every scenario and must be addressed immediately. This study will investigate the efficacy of web-based information security awareness programs from a cross-culture perspective. Subjects from Taiwan and the USA participated in our web-based programs which were created to enhance their security awareness knowledge level. Both pre- and post-tests were given in order to assess whether these aforementioned cultures would be more receptive to the use of technology-driven security awareness programs.

2. Literature review

2.1 The importance of designing a culturally-aware security awareness training program

Culture is the "collective programming of the mind" to distinguish among people of different countries, according to social anthropology theories (Hofstede, 1991, p. 25). Culture is also defined as the habitual method of doing things over time. Therefore, culture is the product of learning, rather than of inheritance (Hofstede, 1993). Competitive strategies, educational systems, training approaches, symbols, values, perceptions of job security (Probst and Lawler, 2006), choice of IT applications (Agrawal *et al.*, 2003) and managerial approaches are a few manifestations of national culture within an organization. Culture influences also include acceptable ways to process information, such as labeling, languages, and symbols (Triandis, 1991). Moreover, culture defines an individual's societal role and prescribes guiding principles to security threats reactions.

The culture has influenced the formation of many security measures, such as national security policy, information ethics, security training, and privacy issues. According to Floridi (2006), privacy as an example is more oblivious to people in the collectivism society than to people in the individualism society. For instance, one study indicated that the German people view privacy is an instrument to protect one's private autonomy and to give that person the freedom to express one's will (Ess, 2006). To people in Hong Kong and China privacy protection does not mean that citizens have the right of being autonomous. As a result, Chinese citizens in those two countries enjoy comparatively limited protection of data privacy in the area of e-commerce, in comparison with Germans and Americans. Therefore, it is imperative to incorporate the culture into the design of IT applications (e.g. security awareness training systems) in order to improve their perceived values (Agrawal *et al.*, 2003) and adoption (Montealegre, 1998).

Many security concerns are common to users worldwide. However, the importance of security concerns varies with countries. For instance, training to increase the awareness of intellectual property is more important in developed countries than in developing countries. As an example, the New York State Parent Teachers Association in the USA is actively raising the security awareness of creating a safe, family-friendly internet environment both inside and outside of the home (PR Newswire, 2007). Countries of the world establish different codes of conduct related to the use of information and communication technologies in order to improve IS security awareness and ethics (Bia and Kalika, 2007). The increase of security awareness and cautious behavior at the individual-level can improve the information security performance of an organization (Albrechtsen, 2007). Thus, the focus of security awareness training must be developed according to the needs of users in different countries and cultures.

2.2 Situational learning to improve security awareness

The "human" factor is the weakest link in information security and the cause of many security threats, according to NIST-SP-800-50 (Wilson and Hash, 2003). Most users do not have adequate security traits and are not sensitive to information security threats in their surrounding environment. An organization can potentially protect itself from security threats by simply improving a user's level of security awareness in their working environment.

The design of an effective information security awareness program needs to solicit user opinions and increase the degree of user involvement (Albrechtsen, 2007). Unclear security requirements of users can result in the confusion between security requirements and architectural security mechanisms from the systems development perspective (Tondel *et al.*, 2008). Consequently, users may learn security awareness topics in general, rather than apply them in their surroundings to secure themselves and their organizations if their roles and security requirements are not clearly specified. Security awareness is role-based learning, detailing the roles and responsibilities of a user in the use of IT systems within an organization. Through the use of training and education users can learn the necessary skills and knowledge to perform IT security control activities.

Situational awareness makes users aware of their surroundings as well as the environmental elements and their contextual meanings (Endsley, 1995). Facilitating this awareness in their working environment allows users to form a mental model to

both understand the current risks of a situation and to predict and possibly prevent the potential adverse effects of these risks. Mental models are "mechanisms whereby humans are able to generate descriptions of system purpose and form, explanations of system functioning and observed system states, and prediction of future states" (Rouse and Morris, 1985, p. 7). A complete mental model of security awareness is to be aware of different forms of security threats, understand how these threats work and predict potential outcomes of allowing them to continue. The awareness is about the perceptions of security threats, since not all of them are so obvious. A user with a higher security awareness level can better sense impending security threats. Laptop theft and run-of-the-mill virus infections are two typical security incidents that can easily be prevented and minimized if users learn to lock their computer and use anti-virus software to check suspicious emails. These two security incidents alone account for US $20 million of loss, according to a 2006 Computer Security Institute/US Federal Bureau of Investigation survey with 131 respondents (Gordon *et al.*, 2006).

This is the rudimentary form of a mental model that can be derived from the situational awareness-learning program. Perceptions can arouse interest, thereby leading to a greater understanding about how the identified threats function. Comprehension is the second level of learning outcomes resulting from situational learning programs. Previous knowledge or experience that is related to the environment can help more efficiently form a coherent mental model of the studied subjects (Dominguez *et al.*, 1994) and take appropriate plan of actions to cope with situations (Sarter and Woods, 1991; Fracker, 1991). Situational training based on scenarios enables users to accumulate learning experience and respond to security threats. Situational learning is an effective user-centered learning approach that improves the perception, comprehension and projection ability of users to secure their surroundings (Endsley and Garland, 2000).

2.3 Cultural influence to the design of security awareness programs as work systems

Technical and social systems can contribute to and are included in the formation of a work system (Schoderbek *et al.*, 1985). The inputs of socio-technical systems include processes, tasks, and technology (Kavan *et al.*, 1999), whereas those of social systems deal with intangible attributes of members within the work systems. Intangible attributes include values, skills, and attitudes. Culture influences both sub-systems. To optimize the functions of the work system, both sub-systems also need to be optimized based on the cultural differences. A work system that is effective in one culture does not necessarily guarantee its effectiveness in other cultures (Hofstede and Bond, 1988). A cursory examination of the popular mobile music applications adopted across countries shows that more than 60 percent of cellular phone users in Korea regularly use these applications, but less than 20 percent of American users are doing so (Wireless Asia, 2005). Mobile gamblers from Asia Pacific and Europe represent more than 75 percent of mobile gambling expenditures among other countries of the world (Gibson, 2006). All these evidences clearly indicate that both technical and social systems need to be considered in order to help better understand how to optimize their synergy (Huse and Cummings, 1985). Incorporating the cultural element into the design of a technical system can increase the odds of designing a more secure system.

Situational security awareness training immerses an individual into his/her familiar environment to improve the efficiency of processing information. To successfully

implement the training, it is important to align the cultural factors (values, beliefs, and assumptions) of users with the managerial practices (Hofstede, 1993; Kirkman and Shapiro, 1997). Therefore, it is plausible that situational security awareness training is a more efficient alternative than the traditional face-to-face training in improving security awareness levels.

The focus of this study is to investigate whether or not situational security awareness training is culturally-bounded. Important exploratory directions are to understand:

- whether people from a particular culture are more receptive to this training approach than people from another culture; and
- which cultural dimension plays an important role to moderate or mediate users' learning performance receiving this training approach in order to improve their security awareness levels.

2.4 Security awareness levels of general users vary with four cultural dimensions

Hofstede (1993) study on the four intercultural dimensions of individualism, power distance, masculinity and uncertainty avoidance lays the groundwork for many social studies that are interested in learning cultural impacts on their areas, ranging from education, politics, economics, motivation patterns, leadership, conflict resolutions (Hoppe, 2004), to innovations adoption (Van Everdingen and Waarts, 2003). Each dimension is measurable with a specific indicator. A high individualism indicator (IDV) pertains to a culture in which in-group relationships are weak and not cohesive. USA (IDV ¼ 91), Australia (90), and Great Britain (89) are in the extreme of high individualism cultures, whereas Taiwan (17) and Guatemala (6) are in the other extreme of low individualism or high collectivism cultures. A high power distance indicator (PDI) pertains to a culture in which the tolerance level of social inequality is higher. Countries in the category of high PDI include Malaysia (PDI ¼ 104), Mexico (81), and India (77). Low PDI cultures include Austria (11), Israel (13), and Ireland (22). A high masculinity indicator (MAS) pertains to a culture in which men are decision-makers and more assertive. A low MAS pertains to a culture in which gender is seen as more neutral in nature. High MAS cultures include Japan (MAS ¼ 95), Austria (79), where as low MAS cultures are Sweden (5) and Denmark (16). A high uncertainty avoidance indicator (UAI) pertains to a culture in which people feel unsafe and has urgent need for structured and written rules to avoid uncertainty. High UAI cultures include Greece (UAI ¼ 112), Japan (92), and France (86), whereas low UAI cultures include Singapore (8) and Denmark (23).

People in different cultures have different levels of security sensitivity depending upon their social and technical environments. These socio-technical backgrounds have resulted in the formation of varying security awareness levels of general users of security risks. Due to differences in information communications and telecommunication infrastructure, varying forms of security risks (e.g. external, internal, virtual, physical, and natural risks) have been formed and adapted. This has gradually shaped the way public users perceive and respond to security threats.

Table I maps organizational and individual security awareness levels with Hofstede's four cultural dimensions: individualism, power distance, masculinity, and uncertainty avoidance. The mapping exercise is our attempt to show potential correlation between cultural dimensions and the security awareness levels at both

individual and organizational levels based on literature review. This observation can provide us a certain degree of confidence in proposing our propositions and hypotheses in the following section. Taking the IDI dimension as an example, individuals in high IDI cultures are self-oriented and they believe in individual decisions and are encouraged to take initiatives (McCoy *et al.*, 2005). Security awareness is a user-involvement exercise as previous evidences indicated. As such, high IDI individuals care about their personal privacy and know that the government has little roles to play in protecting personal privacy. They know the increase of security awareness is their personal responsibility. In contrast, personal privacy right needs to be yielded to government if the collective interests of the society as a whole are greater than the personal privacy. The Peoples Republic of China government requested the cooperation of multinational enterprises, such as Google, to release personal communication records about an individual citizen suspected of violating national interests. These two examples show a clear contrast that individual security awareness level is higher in the high IDI culture than in the low IDI culture.

However, organizational security awareness levels could be providing a contrary evidence because low IDI individuals know that the organization or the government that they work for are monitoring all suspicious activities. The centralized control of personal privacy entrusts an organization with more confidence in controlling and managing each individual in order to optimize the collective interests. Therefore, organizational security awareness levels in the low IDI culture can be relatively higher than in the high IDI culture.

In the realm of security management, individualism and power distance are two salient cultural dimensions that go hand-in-hand. In addition, they each can have potential influence on the security awareness levels at both individual- and organizational-levels but we choose to focus our investigation on determining if the IDI cultural dimension has any particular influence on the effectiveness of security awareness training programs.

2.5 High individualists have a higher individual, but lower organizational security awareness level

To validate our propositions that information security awareness levels of people vary with their culture, we first examine the relationship between the individualistic culture and security awareness level. The goal of this study is to propose hypotheses to test if situational security awareness programs have varying effects on the improvement of security awareness levels of general users. If so, are people from high individualistic

	Organizational security awareness level		Individual security awareness level	
	High	Low	High	Low
IDI (individualism)		X	X	
PDI (power distance)	X			X
MAS (masculinity)	X		X	
UAI (uncertainty avoidance)	X		X	

Table I. Organizational vs individual security awareness levels along four culture dimensions

cultures more receptive to situational awareness training programs than people from low individualistic culture?

Individualists (Americans) react more positively to job insecurity, whereas collectivists (Chinese) react negatively (Probst and Lawler, 2006). President Bush's plan to privatize the social security system was deeply rooted in the individualism culture, according to the Democratic senator Max Baucus (Harrington, 2005). Online behaviors are another form of individualism-collectivism culture. Collectivists (e.g. Japan and Turkey) have a predisposition to associate security issues with financial risks, whereas individualists (USA, UK, and Denmark) are inclined to accept security as a part of products or services (including quality, convenience and satisfaction) or privacy issues (Kucuk, 2002). For this reason, collectivists are less receptive to online individual banking, because its perceived risks are higher than traditional physical banking (Charbaji and Jannoun, 2005).

The influence of individualism culture has altered the perceptions of security and technology to secure individual and organizational assets. Individualists have a higher tolerance of risks and are more willing to adopt security technology. In comparison with the traditional F2F training approach, situational awareness training is a more innovative and unproven approach. Individualists are more likely to perceive the usefulness of this training approach and appreciate its potentials However, at the organizational level; individualists need to work collectively in order to cope with security risks. When asked to try new security training approaches, it is very likely that low individualists resist the adoption of this technology because they consider the adoption as part of individual responsibilities.

The purpose of security awareness programs is to strengthen the "people" factors as the weak point of information security and a primary link to many security threats (Wilson and Hash, 2003). Users who are not sensitive to guard and dissuade information security threats in their surrounding environment can put the entire organization at risk. An immediate measure to toughen the "people" link is to improve three levels of security awareness of general users. Unlike training and education, the purpose of security awareness is to instill the skills into users to perform IT security control activities. Rather, users need to first be aware of security vulnerabilities in their surroundings, and then predict future happenings of security incidences due to these vulnerabilities, and then take actions to resolve security breaches if they happen (Endsley, 1995). In other words, an effective security awareness program can lead users in forming a mental model to understand the present state of the security risks. Moreover, users are able to predict potential adverse effects of these risks and to minimize these effects should they surface. These three levels of security awareness can be increased in the ordered manner via an effective security awareness program.

The effectiveness of the situational training approach adopted in this study to improve these three levels of security awareness can potentially vary the degree of individualism culture because of the unique nature of "felt-involvement" embedded in this training approach. Situational and intrapersonal are two important elements of the "felt-involvement" feature (Richins and Bloch, 1986). Situational awareness training is to deliberately create a "felt-involvement" learning atmosphere so that users can easily immerse themselves into the security situations. The atmosphere of customer involvement is an effective agent for customer acquisition and retention in the

Marketing arena, and the improvement of customer's purchasing intention (Batra and Ray, 1986). A coherent mental model about the studied subjects can be further constructed in the minds of users to ease the comprehension process (Dominguez *et al.*, 1994).

We suspect that high individualists are more likely to be receptive to situational awareness learning than low individualists because the "felt involvement" feature creates less cognitive pressure on learners and ease the comprehension process. As the comprehension process is improved, projection and actions-taking process can be enhanced correspondingly. We therefore propose the following hypothesis:

H1. Security awareness levels.

H1a. High individualists have a higher first level of security awareness than low individualists after receiving the situational training approach.

H1b. High individualists have a higher second level of security awareness than low individualists after receiving the situational training approach.

H1c. High individualists have a higher third level of security awareness than low individualists after receiving the situational training approach.

3. Research methodology

This study used Macromedia Flash as the application to develop an animation-based security awareness program based on Endsleys' (1995) Situational Awareness Dynamic Decision Making Model and Situation Awareness Global Assessment Techniques. Experimental sessions were conducted with 160 Taiwanese and 100 American subjects to assess if culture is a relevant element to be considered when adopting situational security awareness programs. To understand the moderating effect of culture, we compared results collected from two separate studies in the USA and Taiwan with respect to the impact of situational vs traditional security awareness programs on the improvement of three levels of security awareness. This manipulation control makes it possible to detect the effects of the single independent variable (training method) on training outcomes. With the training method as a control factor, any significant differences between these two studies indicate that the exogenous factors of computer self-efficacy, pre-test security awareness levels, and culture exist.

3.1 Course materials

Two security awareness topics were popular with general users: password usage and desktop security. A user needs to know how to create a strong password which would consist of a combination of a certain length, numbers, alpha characters, upper and lower case letters as well as the need to make frequent changes to protect his/her password.

The scope of desktop security includes the use of screen savers, preventing the viewing of information on a computer screen, battery backup devices, and access control, according to NIST-SP-800-50. The authors developed course materials concerning the two aforementioned topic areas while narrowing our research only to one subtopic from each area:

- creating a secure password (Figure 1); and
- protecting the physical assets of information that may appear on a desktop.

A situational learning environment was created that would allow the deliverance of these two subtopics (Figure 2).

3.2 *Measurement design*

The measurements of this study are comprised of an evaluation of computer efficacy and three levels of information security awareness. A pretest was conducted to assess participants' computer efficacy with the survey questionnaire instrument including questions related to computer-related knowledge and existing security awareness levels. After participants received learning sessions, they participated in a post-test to assess their learning performance in each of the three levels of security awareness. Two security experts who are certified with BS7799 security management certificates and two scholars who teach information security courses were invited to modify the survey questionnaire. Native US speakers assisted with the translation of course,

Figure 1.
Creating a secure password

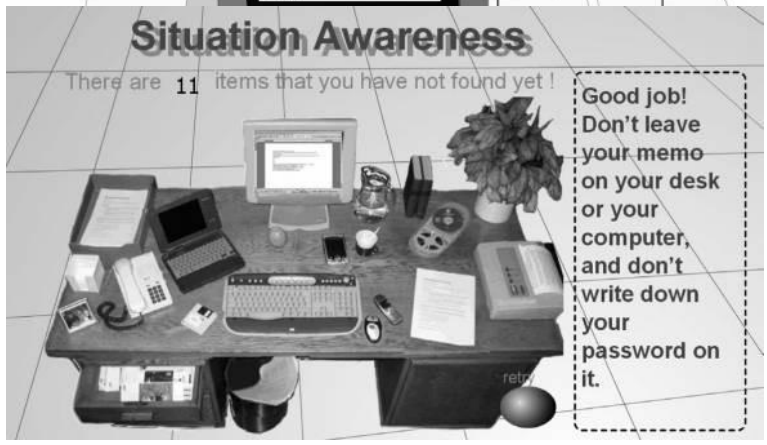

Figure 2.
Protecting physical assets of information on a desktop

materials from Chinese to English in order to accommodate the needs of the American students.

Two groups of college students were exposed to situational and traditional face-to-face learning approaches to assimilate security awareness topics. Three levels of learning outcomes were measured at the end of a one-hour learning session.

In order to clearly understand if the training approach contributes to the difference in learning outcomes, subjects were also required to fill out survey questionnaires to self-report their computer self-efficacy and prior experiences related to security training. In addition, subjects are given a scenario to assess their response actions to security threats.

3.3 Experimental subjects and procedures

One hundred and sixty sophomores from a private university in Taiwan participated in the first round of this study. Another one hundred juniors from a public state university in the USA attended the second round. We deliberately compared the US with Taiwanese subjects because American subjects are high individualists (IDV ¼ 91) and Taiwanese subjects are low individualists (IDV ¼ 17). The intent of this design is to increase the effect size so as to help us control the magnitude of moderating influence of the individualism culture on the relationship between situational awareness and learning outcomes. Effect size is a family of indices to measure the magnitude of influence of a treatment effect (Lipsey and Wilson, 1993). Each group of subjects was equally divided into one of two groups: experimental or control group. Subjects from the experimental group received the situational learning while other subjects from the control group received the traditional face-to-face learning method. Instructors used Microsoft PowerPoint to present the same course materials used in the flash-based situational learning in slides. It has been commonly known that the learning outcomes of face-to-face instructions can largely depend upon the instructor. We took this potential effect into consideration and had the same instructor lecture students in the face-to-face instruction mode for American and Taiwanese subjects, respectively. The "felt-involvement" feature is missing from this step-by-step instruction. For instance, the instructor first explained what constitutes a weak password in a presentation slide. Then the instructors enlisted all passwords that are considered as a weak control, such as using their birthday as a password, not mixing alpha characters with numbers, and writing down passwords and sticking them on a computer screen. Instructors further provided instructions on how to secure passwords and suggested some actions to reset passwords if they were lost. Tables II and III show the distribution of subjects receiving situational or face-to-face training at Taiwan and the US sites, respectively. American subjects were not equally divided because we randomized these two treatments by class. Four classes participated in this study, with a total of 40 students of two classes receiving situational learning and a total of 60 students of two other classes receiving the traditional face-to-face instruction. All subjects received 30 min sessions. This counter-group design can help identify if a situational learning approach is better than a traditional F2F learning approach at improving the level of security awareness for general users.

Group	Number of subjects	Pretest	Learning approach	Post-test
Experimental group (situational training)				
MIS major	40	Computer efficacy	Situational learning	Information security awareness measurements Scenario
International business major	40			
Control group				
MIS major	40	Computer efficacy	Traditional F2F	Information security awareness measurements
IB major	40			Scenario

Table II.
Experimental design at the Taiwan site

Group	Number of subjects	Pre-test	Learning approach	Post-test
Experimental group				
Business major	40	Computer efficacy	Situational learning	Information security awareness measurements
Control group				
Business majors	66	Computer efficacy	Traditional F2F	Information security awareness measurements

Table III.
Experimental design at the US site

4. Statistical data analysis

4.1 Pre-test analysis

Table IV shows that both the experimental and control groups at the Taiwan site are not significantly different related to general computer efficacy. However, subjects in the experimental group appear to have a significantly higher level of security awareness than subjects majoring in International Business with the p value 0.000 (, 0.01).

In contrast, at the US site Table V also detects a significant difference between the situational learning group and traditional learning group in the security awareness level. The computer efficacy in general does not vary very much between the experimental and control groups. Samples from both the US and Taiwan sites have many resemblances. This commonality of the experimental setting in both countries is

	Sample size	Computer efficacy Mean	SD	Security awareness Mean	SD
Experimental group	80	25.50	4.27	30.20	2.83
Control group	80	24.55	3.86	25.46	4.64
Levene test	F	0.325		11.783	
	p-value	0.569		0.001***	

Notes: p , 0.05 (*) significant; p , 0.01 (**) very significant

Table IV.
t-test analysis for low individualists (Taiwanese)

a good control to assess if different training approaches can enlarge the differences in training outcomes. It should be noted that the experimental group in both countries tend to have a higher security awareness level before receiving situational trainings. The constraint may aggravate the researching findings in either direction, such as situational training is very effective or not ineffective. However, if the researching findings at both sites go to the opposing direction our argument to either support or reject the usefulness of situational security awareness training to high individualists is more convincing. With this logic in mind, the following section will examine the learning outcomes after having experimental and control groups receive situational and traditional security awareness training.

4.2 *Post-test analysis*

Table VI indicates that after receiving either situational or traditional security awareness training, no significant differences in all three levels of security awareness exist between the two groups at the Taiwan site. This indicates that situational learning does not deliver its anticipated benefits in improving general users' perception, comprehension and projection ability. Control groups that received the traditional training approach can perform as well as the experimental groups that are equipped with better security awareness before the training session took place. In contrast, situational security awareness training at the US site does help the experimental group surpass the control group in the measurements of all three security awareness levels (Table VII).

The Anova test (Table VII) shows that these three performance metrics are all significant (p ¼ 0.000 for perception; p ¼ 0.007 for comprehension; and p ¼ 0.009 for projection). This indicates that the group of subjects receiving situational awareness

		Computer efficacy		Pre-test awareness	
	Sample size	Mean	SD	Mean	SD
Experimental group	34	6.38	0.70	5.69	0.59
Control group	66	5.95	0.90	5.26	0.70
Levene test	F	0.001		9.56	
	p-value	0.978		0.003 **	

Notes: p > 0.05 (*) significant; p > 0.01 (**) very significant

Table V.
t-test analysis for high individualists (Americans)

	Group	Size	Mean	SD	Levene test		*t*	*p*
Post-test awareness								
SA1	Experimental	80	25.61	3.79	2.121	0.147	20.255	0.799
	Control	80	25.48	2.99				
SA2	Experimental	80	24.35	4.28	0.003	0.957	21.333	0.184
	Control	80	23.46	4.14				
SA3	Experimental	80	28.53	3.27	0.96	0.757	20.539	0.590
	Control	80	28.25	3.18				

Notes: p > 0.05 (*) significant; p > 0.01 (**) very significant

Table VI.
Measures of dependent variables between experimental and control groups at Taiwan site

training outperformed the traditional group. In addition, the situational awareness training approach is indeed a more effective training approach than the traditional approach at helping general users improve their security awareness levels.

5. Discussion

American users who received the situational security awareness training outperformed those who received the traditional step-by-step instruction. In contrast, Taiwanese users of both experimental and controllable groups had similar performances after receiving respective training approaches. Since the research findings at both sites go in the opposing direction, we are confident in stating that situational security awareness training is more useful and effective to high individualists than high collectivists.

As seen below in (Table VIII), *H1a-H1c* are supported in the US site, whereas those hypotheses were rejected in the Taiwanese site.

These findings confirm the potential influence of the individualism culture as a socio-technical factor concerning the improvement of knowledge surrounding the topic of security awareness. Our study further suggests that the cultural trait, particularly the individualism cultural dimension, is a strong dispositional predictor of the efficacy of situational training applied in the context of security awareness improvement.

Table VII. Measures of dependent variables between experimental and control groups at the US site

	Group	Size	Mean	SD	*F*-value	*p*
Post-test awareness						
SA1	Experimental	34	6.30	0.74	13.40	0.000 **
	Control	66	5.70	0.80		
SA2	Experimental	34	6.27	0.58	7.568	0.007 **
	Control	66	5.84	0.83		
SA3	Experimental	34	6.45	0.62	7.15	0.009 **
	Control	66	6.06	0.72		

Note: $p < 0.05$ (*) significant; $p < 0.01$(**) very significant

Table VIII. Summary of hypotheses testing

Security awareness levels	Hypotheses	US site	Taiwan site
SA2	*H1b.* High individualists have a higher second level of security awareness than low individualists after receiving the situational training approach	Supported ($p = 0.007 < 0.01$)	Rejected ($p = 0.184 > 0.05$)
SA3	*H1c.* High individualists have a higher third level of security awareness than low individualists after receiving the situational training approach	Supported ($p = 0.009 < 0.01$)	Rejected ($p = 0.590 > 0.05$)

The positive influence of the individualism culture also corroborates with the finding in the field of consumer behavior that high individualists have a higher intention than high collectivists to purchase personalized products in an online retailing situation (Moon *et al.*, 2008). This culture trait also exhibits its influence on the trust formation. For instance, a trustee's perceived ability and integrity are the source of trust to individualists and predictability as benevolent interactions are to collectivists (Branzei *et al.*, 2007). The positive correlation between individualism culture and the efficiency of situational awareness programs has some commonalities between the topics of cultural traits and the acceptance of consumer goods, which in fact involves the fast formation of trust.

It makes no significant difference for collectivists to receive either situational awareness or step-by-step instruction. However, situational awareness programs make individualists aware of their surroundings as well as the environmental elements and their contextual meanings in a more efficient and effective manner. Situational awareness programs are also an effective vehicle to help individualists form a mental model to both understand the current risks of a situation and to predict and possibly prevent the potential adverse effects of security risks and vulnerabilities.

We administered a pre-test for both American and Taiwanese subjects before they were exposed to both the situational awareness and traditional face-to-face treatments. The purpose of this pre-test was to evaluate and minimize the impacts of extraneous factors, such as age differences, computer efficacy, experience, ethnical heterogeneity or family profiles. Students from universities in both the US and Taiwan are either juniors or seniors. They are all full-time students, with the studied American students in a public university and the Taiwanese students in a private university. About 99 percent of American students are Caucasian, and 100 percent of students from Taiwan are native Taiwanese. Therefore, the potential impact of ethnical diversity is minimal. It is highly probable that all the variables this study deliberately controlled have negligible effects on learning outcomes. We are confident that the impact of individualism culture on the efficacy of situational awareness learning does exist and needs to be paid attention to.

6. Conclusions and future research

Security awareness is an important issue that all individuals must be concerned with as information is transferred around the globe. Global citizens also react differently to security awareness as would be expected due to differing cultures and the emphasis that is placed on individualism. Certainly, awareness of the risks and safeguards is the first line of defense that can be employed by any individual, but how individuals address these risks can be very dissimilar in different cultures.

Through the use of different testing results at Taiwan and the US sites, the present cultural implications and opportunities for suggest future research. As we have seen, low individualists appear less receptive to situational awareness training than high individualists. More specifically, high individualists have a higher level of security awareness than low individualists after receiving situational training.

For other cultures the question and future research remains "How do we best or most effectively train individuals in relation to security awareness?" Though the answer is currently not known within the international arena, more research may be able to provide this answer.

References

Albrechtsen, E. (2007), "A qualitative study of user's view on information security", *Computers & Security*, Vol. 26 No. 4, p. 276.

Agrawal, V.K., Haleem, A. and Sushil (2003), "Successful implementation of business process reengineering and computer based information systems: awareness and training program (NIST SP 800-50)", *National Social Science Journal*, Vol. 20 No. 2, pp. 1-16.

Batra, R. and Ray, M.L. (1986), "Situational effects of advertising repetition: the moderating influence of motivation, ability, and opportunity to respond", *Journal of Consumer Research*, Vol. 12, pp. 432-45.

Bia, M. and Kalika, M. (2007), "Adopting an ICT code of conduct: an empirical study of organizational factors", *Journal of Enterprise Information Management*, Vol. 20 No. 4, p. 432.

Branzei, O., Vertinsky, I. and Camp, R.D. (2007), "Culture-contingent signs of trust in emergent relationships", *Organizational Behavior & Human Decision Processes*, Vol. 104 No. 1, pp. 61-82.

Charbaji, A. and Jannoun, S.E.L. (2005), "Individuality, willingness to take risk, and use of a personal e-card: a Lebanese study", *Journal of Managerial Psychology*, Vol. 20 No. 1, pp. 51-8.

Dominguez, C., Vidulich, M., Vogel, E. and Mcmillan, G. (1994), *Situation Awareness: Papers and Annotated Bibliography*, Armstrong Laboratory, Human System Center.

Endsley, M. (1995), "Measurement of situation awareness in dynamic systems", *Human Factors*, Vol. 37 No. 1, pp. 65-84.

Endsley, M. and Garland, D. (2000), *Experimental Analysis and Measurement of Situation Awareness*, Embry-Little University Press, Daytona Beach, FL.

Ess, C. (2006), "Ethical pluralism and global information ethics", *Ethics and Information Technology*, Vol. 8 No. 4, pp. 215-26.

Filipek, R. (2007), "European nations make security a high priority", *The Internal Auditor*, Vol. 64 No. 5, pp. 15-17.

Floridi, L. (2006), "Four challenges for a theory of information privacy", *Ethics and Information Technology*, Vol. 8 No. 3, pp. 109-19.

Fracker, M. (1991), *Measures of Situation Awareness: Review and Future Directions*, Armstrong Laboratories, Wright Patterson Air Force Base, OH.

Gibson, B. (2006), "Mobile is ideal channel for casual gambling", *New Media Age*, p. 7.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Richardson, R. (2006), *2006 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute.

Grant, I. (2007), "DaimlerChrysler security drive targets 360,000 staff", *Computer Weekly*, p. 4.

Harrington, J. (2005), "Sen. Baucus relishes resisting Bush's social security privatization plan", *Knight Rider Tribune Business News*, August 16.

Hofstede, G. (1991), *Cultures and Organizations: Software of the Mind*, McGraw-Hill, London.

Hofstede, G. (1993), "Cultural constraints in management theories", *Academy of Management Executive*, Vol. 7 No. 1, pp. 81-94.

Hofstede, G. and Bond, M. (1988), "The confucius connection: from cultural roots to economic growth", *Organizational Dynamics*, Vol. 16 No. 4, pp. 4-21.

Hoppe, M. (2004), "Introduction: Geert Hofstede's culture's consequences: international differences in work-related values", *Academy of Management Executive*, Vol. 18 No. 1, pp. 73-4.

Huse, E.F. and Cummings, T.G. (1985), *Organization Development and Change*, West, New York, NY.

Kavan, C.B., O' Hara, M.T., Patterson, E.C. and Bostrom, R.P. (1999), "Excellence in client/server information system implementations: understanding the STS connection", *Management Decision*, Vol. 37 No. 3, pp. 295-304.

Kirkman, B.L. and Shapiro, D.L. (1997), "The impact of cultural values on employee resistance to teams: towards a model of globalized self-managed work teams effectiveness", *Journal of International Business Studies*, Vol. 22 No. 3, pp. 730-57.

Kucuk, S.U. (2002), "The changing consumerism with the internet: a global perspective", *Journal of Euro – Marketing*, Vol. 12 No. 1, p. 41.

Lipsey, M.W. and Wilson, D.B. (1993), "The efficacy of psychological, educational, and behavioral treatment: confirmation from meta-analysis", *American Psychologist*, Vol. 48, pp. 1181-209.

McCoy, S., Galletta, D.F. and William, R. (2005), "Integrating national culture into IS research", *Communications of AIS*, Vol. 2005 No. 15, pp. 211-24.

Montealegre, R. (1998), "Managing information technology in modernizing 'against the odds': lesson from an organization in a less-developed country", *Information & Management*, Vol. 34, pp. 103-16.

Moon, J., Chadee, D. and Tikoo, S. (2008), "Culture, product type, and price influences on consumer purchase intention to buy personalized products online", *Journal of Business Research*, Vol. 61 No. 1, pp. 31-9.

PriceWaterHouseCoopers (2006), "Information security breaches survey 2006", available at: www.pwc.com/uk/eng/ins-sol/publ/pwc_dti-fullsurveyresults06.pdf (accessed November 24, 2007).

PR Newswire (2007), "Blue coat and New York State PTA to raise awareness on child internet safety; joint initiative launched in recognition of cyber security awareness month to educate members, parents and community on the impact of internet dangers", *PR Newswire*, New York, NY.

Probst, T.M. and Lawler, J. (2006), "Cultural values as moderators of the outcomes of job insecurity: the role of individualism and collectivism", *Applied Psychology: An International Review*, Vol. 55, pp. 234-54.

Richins, M. and Bloch, P.H. (1986), "After the new wears off: the temporal context of product involvement", *Journal of Consumer Research*, Vol. 13, pp. 280-5.

Rouse, W.B. and Morris, N.M. (1985), *On Looking into the Blackbox: Prospects and Limits in the Search for Mental Models (DTIC#AD-A159080)*, Center for Man-Machine Systems Research, Georgia Institute of Technology, Atlanta, GA.

Sarter, N. and Woods, D. (1991), "Situation awareness: a critical but ill-defined phenomenon", *International Journal of Aviation Psychology*, Vol. 1, pp. 45-7.

Schoderbek, P.P., Schoderbek, C.G. and Kefalas, A.G. (1985), *Management Systems: Conceptual Considerations*, 3rd ed., Business Publications, Plano, TX.

Tondel, I.A., Jaatun, M.G. and Meland, P.H. (2008), "Security requirements for the rest of US: a survey", *IEEE Software*, Vol. 25 No. 1, p. 20.

Triandis, H.C. (1991), *Cross-cultural Industrial and Organizational Psychology*, Consulting Psychologists Press, Inc., Palo Alto, CA.

Van Everdingen, Y.M. and Waarts, E. (2003), "The effect of national culture on the adoption of innovations", *Marketing Letters*, Vol. 14 No. 3, pp. 217-32.

Wilson, M. and Hash, J. (2003), *Building an Information Technology Security Awareness and Training Program*, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD.

Wireless Asia (2005), "Hefty appetite for music on cellphones", available at: www.telecomasia.com (accessed November 14, 2007).

Further reading

CSI/FBI (2006), "Computer crime and security survey", Computer Security Institute, available at: www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml (accessed November 13, 2007).

Gomez, C., Kirkman, B.L. and Shapiro, D.L. (2000), "The impact of collectivism and in-group/out-group membership on the evaluation generosity of team members", *the Academy of Management Journal*, Vol. 43 No. 6, pp. 1097-106.

Richins, M.L., Bloch, P.H. and McQuarrie, E.F. (1992), "How enduring and situational involvement combine to create involvement responses", *Journal of Consumer Psychology*, Vol. 1 No. 2, pp. 143-54.

Corresponding author

B. Dawn Medlin can be contacted at: medlinbd@appstate.edu

This article has been cited by:

1. Sindhuja P N Department of Operations & IT, ICFAI Business School Hyderabad, Hyderabad, India. Anand S. Kunnathur Department of IOTM, University of Toledo, Toledo, Ohio, United States. . 2015. Information security in supply chains: a management control perspective. *Information and Computer Security* **23**:5, 476-496. [Abstract] [Full Text] [PDF]
2. Bukelwa Ngoqo Department of Applied Informatics, Walter Sisulu University, East London, South Africa Stephen V. Flowerday Department of Information Systems, University of Fort Hare, East London, South Africa . 2015. Exploring the relationship between student mobile information security awareness and behavioural intent. *Information and Computer Security* **23**:4, 406-420. [Abstract] [Full Text] [PDF]
3. Fredrik Karlsson CERIS, Department of Informatics, Örebro University, Örebro, Sweden Joachim Åström Political Science Department, Örebro University, Örebro, Sweden Martin Karlsson Political Science Department, Örebro University, Örebro, Sweden . 2015. Information security culture – state-of-the-art review between 2000 and 2013. *Information and Computer Security* **23**:3, 246-285. [Abstract] [Full Text] [PDF]
4. Mohammed A. AlnatheerInformation Security Culture Critical Success Factors 731-735. [CrossRef]
5. Benedikt Lebek Institute for Information Systems Research, Leibniz University of Hannover, Hannover, Germany Jörg Uffen Institute for Information Systems Research, Leibniz University of Hannover, Hannover, Germany Markus Neumann bhn Dienstleistungs GmbH & Co. KG, Hameln, Germany Bernd Hohler bhn Dienstleistungs GmbH & Co. KG, Hameln, Germany Michael H. Breitner Institute for Information Systems Research, Leibniz University of Hannover, Hannover, Germany . 2014. Information security awareness and behavior: a theory-based literature review. *Management Research Review* **37**:12, 1049-1092. [Abstract] [Full Text] [PDF]
6. Sindhuja PN Department of IT and Operations, IBS Hyderabad, a Constituent of IFHE, Deemed to be University, Hyderabad, India . 2014. Impact of information security initiatives on supply chain performance. *Information Management & Computer Security* **22**:5, 450-473. [Abstract] [Full Text] [PDF]
7. Rayne Reid Institute of ICT Advancement, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa Johan van Niekerk Institute of ICT Advancement, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa . 2014. Brain-compatible, web-based information security education: a statistical study. *Information Management & Computer Security* **22**:4, 371-381. [Abstract] [Full Text] [PDF]
8. Rayne Reid, Johan Van NiekerkFrom information security to cyber security cultures 1-7. [CrossRef]
9. Ruey-Shiang Shaw, Huan-Chao Keh, Nan-Ching Huang. 2013. Information Security Awareness On-Line Materials Design with Knowledge Maps. *International Journal of Distance Education Technologies* **9**:4, 41-56. [CrossRef]
10. Shuhaili Talib, Nathan L. Clarke, Steven M. Furnell. 2013. Establishing A Personalized Information Security Culture. *International Journal of Mobile Computing and Multimedia Communications* **3**:1, 63-79. [CrossRef]
11. Sang-Hoon Kim, Sun-Young Park. 2011. Influencing Factors for Compliance Intention of Information Security Policy. *The Journal of Society for e-Business Studies* **16**:4, 33-51. [CrossRef]
12. Princely Ifinedo. 2011. An Exploratory Study of the Relationships between Selected Contextual Factors and Information Security Concerns in Global Financial Services Institutions. *Journal of Information Privacy and Security* **7**:1, 25-49. [CrossRef]

13. Shuhaili Talib, Nathan L. Clarke, Steven M. FurnellAn Analysis of Information Security Awareness within Home and Work Environments 196-203. [CrossRef]
14. Princely IfinedoRelationships between Information Security Concerns and National Cultural Dimensions 134-153. [CrossRef]
15. Shuhaili Talib, Nathan L. Clarke, Steven M. FurnellEstablishing a Personalized Information Security Culture 53-69. [CrossRef]