The Impact Of Information Richness On Information Security Awareness Training Effectiveness

By: R.S. Shaw, **Charlie C. Chen**, Albert L. Harris, & Hui-Jou Huang

Abstract

In recent years, rapid progress in the use of the internet has resulted in huge losses in many organizations due to lax security. As a result, information security awareness is becoming an important issue to anyone using the Internet. To reduce losses, organizations have made information security awareness a top priority. The three main barriers to information security awareness are: (1) general security awareness, (2) employees' computer skills, and (3) organizational budgets. Online learning appears a feasible alternative to providing information security awareness and countering these three barriers. Research has identified three levels of security awareness: perception, comprehension and projection. This paper reports on a laboratory experiment that investigates the impacts of hypermedia, multimedia and hypertext to increase information security awareness among the three awareness levels in an online training environment. The results indicate that: (1) learners who have the better understanding at the perception and comprehension levels can improve understanding at the projection level; (2) learners with text material perform better at the perception level; and (3) learners with multimedia material perform better at the comprehension level and projection level. The results could be used by educators and training designers to create meaningful information security awareness materials.

R.S. Shaw, **Charlie C. Chen**, Albert L. Harris, & Hui-Jou Huang (2009) "The Impact Of Information Richness On Information Security Awareness Training Effectiveness." *Computers & Education* #52 pp. 92–100 [DOI:10.1016/j.compedu.2008.06.011] Version Of Record Available At www.sciencedirect.com

1. Introduction

The perceived threats of security risks and the adoption of behaviors to minimize them are often not synchronized with each other when it comes to employee actions. A survey of more than 1000 teleworkers in 10 countries showed that regardless of the country, teleworkers tend to have a higher level of security awareness than their behavior shows (Wireless News, 2006). Security awareness is the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organization's data and networks. Some risk-prone behaviors that are aggravating security concerns include the sharing of corporate computing resources with non-employees, using corporate computing resources for non-work related tasks (e.g. online shopping), and opening unknown e-mails and attachments. Most surveyed teleworkers receive more security awareness training than non-teleworker office employees and are bounded by corporate policy to secure their work. Despite these efforts, their actual behaviors in securing corporate networks and information are less than adequate. This observation poses two important research questions. First, it is critical to continuously heighten the security awareness (SA) culture in organizations and translate this culture into actual security aware behaviors. Second, most SA training available to date may not be effective to bridge the gap between perception and behavior. Additional training alternatives are needed to more effectively bridge the gap.

The size of networks continues to grow and, along with this growth, there is an increase of security risks. A longitudinal study on SA shows that, over the 2004–2006 time frames, the average loss and the number of reported security breaches were significantly reduced (Lawrence, Loeb, & Richardson, 2006). One major cause of this improvement in security problems is the continuous investment of small and medium sized firms in both information security technology and SA programs (Lawrence et al., 2006). Information technology personnel alone are not effective in stopping security breaches from happening; the security awareness of end users must be improved.

The number of layers of technological defense can be as strong as possible. However, it takes only a minor mistake (e.g. writing passwords on a notepad, leaving the PC on without locking the door) made by a user to undermine sophisticated security technology. Users with low security awareness are one of the weakest security loopholes. A robust awareness program is paramount to ensuring that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them (NIST SP 800-16, 1998). After receiving an effective SA program, the mindset of users should be able to progress from "become aware" to "be aware" to "stay aware" of security threats (Schlienger & Teufel, 2003).

One of the critical success factors of a SA program is the relevance, timeliness, and consistency of security information because information risk profiles never stop changing (Kruger & Kearney, 2006). Equally important is the delivery of the latest security information in different ways (e.g. newsletter, video, seminar and lecture) so that users receive many different messages. As online learning technology makes rapid progress, many of its features (e.g. e-mail broadcasting, online synchronous and asynchronous discussion, information uploading, blogging, animation, and multimedia) appear to be a feasible alternative to deliver SA programs. E-learning systems hold the promise of providing a vehicle for effective delivery of SA programs to everyone in an organization.

Many challenges appear when trying to realize the true efficacy of an online SA program. A major challenge with SA programs is the lack of a fully developed methodology to deliver them (Valentine, 2006). Other challenges may include:

- How should course materials be constructed to reflect the personal needs of a variety of end users?
- How often should the information be updated?
- How does one manage the information to help end users sense the urgency of security breach events?
- How does one combine different features of online learning systems to develop an effective SA program?

The focus of this study was to provide insights on the influence of information richness on the effectiveness of online SA programs. An integrative research model was proposed based on a thorough literature review. Hypotheses were constructed to examine the relationships among constructs of the research model. Media that varied in the degree of information richness were the vehicles to deliver online SA programs. We compared four attributes – feedback compatibility, multiple cues, language variety, and personal focus – of information richness with respect to their influence on learning effectiveness of SA programs. We derived our findings based on statistical analysis of the data. Seven of the eight hypotheses were supported.

2. Conceptual foundations

2.1. The growing importance of a SA program in an organization

In the emerging web savvy society, security vulnerabilities via intense online social activities (e.g. mySpace.com; Facebook.com, blogging, instant messaging, YouTube.com, etc.) are growing exponentially. Users engaging in online activities are equipped with varying and unequal levels of security awareness. This security awareness disparity has resulted in weak lines of "people" defense. Further aggravating the weak line is the continuous evolving of new risks and attacks to elude widely accepted security technology (e.g. virus control, anti-spam software, and firewalls) (Claburn, 2005). As a result, the improvement of security awareness levels of general users needs to be one of today's top security concerns. If not, no matter how much sophisticated security technology is deployed, a small human mistake (e.g. releasing confidential information to malicious attackers; or connecting a corporate laptop to unsecured wireless networks in an airport) can turn these technologies into defenseless targets.

With peer-to-peer and group-to-group interactions becoming online social norms, information security can never be stressed enough. Prominent web-related security risks range from stealing user ids and passwords to classified spamming, to privacy intrusion, to copyright violations. For those users not actively involving in an online social activity, security risks (e.g. identity theft, password protection, etc.) persistently exist. Users with low security awareness are often careless in handling personal and confidential information, which includes the confidentiality, availability and integrity of personal information (Schneider & Therkalsen, 1990). The source of security risks can originate from software, hardware, network, technical skills, and casual computing. It is imperative that an organization trains users to be aware of security risk sources, and take corrective actions if vulnerabilities do occur.

2.2. Major challenges with the existing SA programs in enhancing SA levels of users

Poor security behavior of many users (e.g. user security errors, carelessness, and negligence) has contributed to many security breaches. An increased number of organizations are recognizing the importance of having a SA program in place. Inherent in the success of a SA program is to ensure that employees achieve three levels of awareness of security risks: perception, comprehension and projection. As more employees of an organization make progress along these three levels, the "people" side security can be heightened. The heightening of end user security awareness can help inculcate security cultures and values, thereby developing better security competency. However, the one-size-fits-all approach at both the organization-level and the individual-level has contributed to the varied performance of SA programs (Valentine, 2006). It is essential to have a more consistent methodology to tailor a SA program based on the levels of security awareness to be achieved.

2.2.1. Level 1 SA: perception

The first step towards securing an organization is to sense and detect potential security risks of its business environment. Perception is to achieve an understanding of the presence or awareness of a threat. The odds of forming a correct picture of security threats of the surroundings can be largely enhanced with the improvement of the perception of security awareness. One international firm adopted a phase-based global SA program and gradually rolled out an online and offline SA program. They were able to successfully enhance the perception of security awareness of more than 100,000 employees in 100 countries (Power & Forte, 2006).

2.2.2. Level 2 SA: comprehension

The perception of the presence of security risks is insufficient to counterattack those identified risks. Security risks pose a wide variety of threats to an organization because of their natural differences. It is important for users to comprehend, understand, and assess the dangers posed by different security risks. The emphasis of training to improve the second SA level is to ensure that users know how to integrate information from multiple sources and interpret them in the right direction. More importantly, users need to have the ability to disseminate information that can assist users in combating the security risks in their surrounding environment (Jones & Endsley, 1996). The improvement of user comprehension of security risks can change the way people think about risks and controls. SA at level 2 can further ease the persuasion and argumentation process that is inherent in getting company-wide attention (Highland, 1995).

2.2.3. Level 3 SA: projection

Prevention is better than cure. To prevent potential risks from occurring, end users need to have the ability to project or predict the future course of security attacks. Projection is the third level of improvement in security awareness. The ability to anticipate future situational events indicates that users have the highest level of understanding of their surroundings. Timely decisions can be made with the readiness of the projection ability. In the fields of air traffic control, power plant operations, maintenance, and medicine, most skilled experts are well equipped with the ability to project future conditions (Endsley & Garland, 2000). The ultimate goal of an effective SA program is to prepare users with the ability of projecting potential security risks.

Given the three levels of security awareness, two hypotheses were developed for investigation. They were:

Hypothesis 1: Users with a higher perception level of security risks are more likely to have a higher comprehension level of these risks.

Hypothesis 2: Users with a higher comprehension level of security risks are more likely to have a better ability to project potential security risks.

2.3. E-learning systems as a feasible alternative to deliver SA programs

Many users find existing SA programs boring and ineffective (Leach & Behaviour, 2003). The Web is an ideal vehicle to deliver online SA programs to overcome the learning ineffectiveness. Course materials in digital formats can be so diverse that they can be developed to raise the learning interests of users based on their needs. The retrieval of course materials can be bilateral, between instructor and users, or multilateral, among two or more users. An effective SA program heavily relies on both the "push" and "pull" of relevant and timely security information to and from users. As e-learning systems grow in their sophistication, they hold many possibilities of delivering effective and economic SA programs.

Human computer interface (HCI) is an important element in the design of an effective SA program. Incorporating HCI criteria into the design of SA programs can enhance their user-friendliness and learning effectiveness (Johnston, Eloff, & Labuschagne, 2003). One of the important HCI design criterion that is particularly pertinent to a SA program is the "match between the system and the real world" Nielsen, 2000). As security risks never stop evolving, using real world cases or metaphors would make learning easier, allow understand, and, possibly, help perform security awareness tasks. The Web can easily handle the needs of multimedia (e.g. audio, video and animation) to help reflect real scenarios of security risks. This implies that the information richness of various multimedia could have potential influence on the effectiveness of online SA programs.

2.4. The influence of media richness on the effectiveness of online SA programs

SA programs are gaining popularity in high information richness media, including audio, streaming video, interactive posters, and virtual reality. Information richness refers to the information carrying capacity of media. The capacity or information richness of the media can be increased by manipulating one or more of the following attributes: (1) the medium's capacity for immediate feedback, (2) the number of cues and channels available, (3) language variety; and (4) the degree to which intent is focused on the recipient (Daft & Lengel, 1984). Greater social presence of a medium creates a greater immediacy and warmth of the communication, thereby creating a better learning environment. As one of the four attributes is increased, the ability of the media to carry more information and more effectively change the understanding of users about the studied subjects within a time interval is increased.

Face-to-face meetings are the richest media because they incorporate all of the attributes. Online media are much less in richness when compared to face-to-face meetings. Many online tools are emerging to enhance media richness. For example, instant messaging and e-mail can incorporate emotion icons, audibles, and audio and video transmissions. Blogging services integrate hypertext, pictures, and asynchronous feedback. YouTube.com allows the peer-to-peer sharing of video files. Many real estate companies (e.g. 21th Century and RE/MAX) are leveraging virtual reality to provide a simulated tour of the entire house for prospective buyers. Auto firms are assimilating the 360° of virtual reality to help prospective buyer tour interior and exterior parts of a car. The degree of information richness can possibly explain the wide acceptance of these media.

In the design of an effective online SA program, the importance of information richness can be critical to success. Hypermedia (highest richness), multimedia (middle richness) and hypertext (low richness) are distinct in their degree of information richness, and vary in the order of information richness. These three media are pertinent to our investigation of the influence of information richness on the effectiveness of online SA programs.

2.4.1. Hypermedia

Hypermedia is the richest medium of the three studied. Hypermedia is an interactive medium that can consist of graphics, audio, video, plain text and hyperlinks, intertwined to create a generally non-linear medium of information. Using hypermedia, the user can "jump" to a topic of interest rather than going sequentially through other materials to get to the same topic of interest. The World Wide Web is a classic example of hypermedia. Hypermedia can use concept mapping or knowledge mapping. Concept mapping or knowledge mapping are growing in their popularity to enhance motivation, attention, understanding, and recall of students in the classroom setting (Eppler, 2006). Concept maps arrange major concepts into a visual structure to help users understand major concepts and their interrelationships. This tool

can create a meaningful and active learning process by helping users integrate the existing cognitive structures of learners with new concepts, and thus construct new knowledge (Novak, 1990). Knowledge mapping is an enhanced version of concept mapping. Knowledge maps are a tool to organize ideas, opinions and propositions, and the constitution of knowledge (Anderson, 1983), in a multi-level hierarchical structure to represent mental models to a learner. The proliferation of these technologies illustrates the importance of information richness in the media.

Hypermedia combines text and multimedia. This technology is commonly used to denote a collection of information and multimedia elements that are interconnected by links. Users can easily access relevant information to assist their understanding of security awareness via hypermedia. Hypermedia can be customized to represent the cognitive structure (schema and mental models) of users to ease the process of constructing new concepts. A learner is more likely to have the deep learning or better learning performance when he/she forms a cognitive structure (Bruner, 1966).

2.4.2. Multimedia

Multimedia is the middle medium in richness, in between hypermedia and hypertext. Multimedia combines text, image, sound, music, animation, video and virtual reality, but must be accessed in a linear sequence. The use of multimedia in the classroom has shown its effects on providing personalized learning, encouraging self-expression, giving a sense of ownership, and fostering communications. However, multimedia does not emphasize the arrangement of concepts, so the acquisition process of concepts can be eased. Moreover, multimedia does not provide feedback and interactive capability. Thus, multimedia is weaker than hypermedia in the degree of information richness. The lower degree of information richness in the multimedia, as compared to hypermedia, can potentially result in lower learning effectiveness in the three levels of security awareness: perception, comprehension and projection.

2.4.3. Hypertext

Hypertext is plain text with the hyperlink features that does not incorporate feedback capability, multiple cues, language variety, and personal focus. The absence of these four media richness attributes places hypertext in the low end of the information richness spectrum that we are examining. Thus, hypertext is considered the least effective among these three media in enhancing the security awareness levels of users.

Given these three levels of information rich media – hypermedia, multimedia, and hypertext – six hypotheses were developed for this study. They were:

Hypothesis 3: Hypermedia-based online SA programs are more effective than multimedia-based ones in enhancing the perception of users about security awareness.

Hypothesis 4: Hypermedia-based online SA programs are more effective than multimedia-based ones in enhancing the comprehension of users about security awareness.

Hypothesis 5: Hypermedia-based online SA programs are more effective than multimedia-based ones in enhancing the projection ability of users about security awareness.

Hypothesis 6: Multimedia-based online SA programs are more effective than hypertext-based ones in enhancing the perception of users about security awareness.

Hypothesis 7: Multimedia-based online SA programs are more effective than hypertext-based ones in enhancing the comprehension of users about security awareness.

Hypothesis 8: Multimedia-based online SA programs are more effective than hypertext-based ones in enhancing the projection ability of users about security awareness.

3. Methodology

3.1. Research model

Based on our literature search, a research model, shown in Fig. 1, was developed to examine the eight hypothesized relationships. We used a laboratory experimental methodology to test these eight hypotheses. This research method enabled us to manipulate different training approaches based on the degree of media richness, and to assess their influence on the effectiveness of learning security awareness concepts and skills. Three training sessions were developed. One used hypermedia, a high media richness environment; the second used

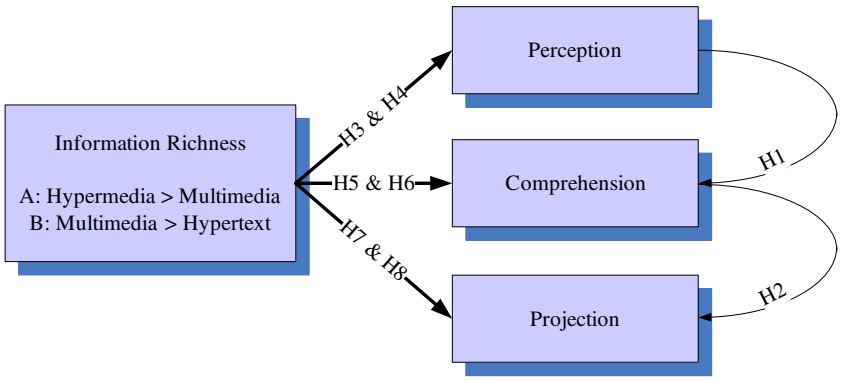

Fig. 1. Research model.

multimedia, a middle media richness environment; and the third used hypertext, a low media richness environment. Effort was made to make each session as comparable as possible. They covered the same security awareness topics. Presentation of the material was as comparable as possible across the three media. Great effort was made to ensure that the material covered was the same in all three training sessions.

3.2. Operational procedure

We first conducted a pretest to ensure users participating in the two experiments had comparable level of security awareness. Users exceeding the average security awareness level were considered experienced users in the area of security awareness and were excluded from participating in the full-scale study. The remaining subjects continued to participate in the experiment. They were randomly assigned to one of the three training sessions – hypermedia (high media richness), multimedia (middle media richness), and hypertext (low media richness). Depending on the group assigned, subjects visited different websites to study course materials for one week. After studying the course materials, students participated in a post-test to assess their learning performance in the three security awareness levels – perception, comprehension and projection.

3.3. Subjects' background

The sample consisted of a total of 240 freshmen from four MIS classes at a private university in Taiwan who were taking an introductory MIS course. Seventy-three students were absent in the pretest. Thirteen responses were invalid in the pretest. After excluding these 86 subjects from the population, 154 students continued into the full-scale experiments. To mitigate the effect of unequal cell size, we randomly eliminated one student from the remaining population. This allowed us to evenly assign 51 students to each experimental group.

3.4. Course material

There are 30 information security awareness topics, according to National Institute of Standards and Technology Special Publication 800-50 (Wilson &Hash, 2003). Those topics range from password usage and management, to protection from viruses and other malicious code, to social engineering and suspicious e-mail attachments. Among these topics, e-mail management is one of the weakest areas because of the large number of people who use e-mail. We, therefore, designed our course materials along this security awareness topic. We deliberately developed the course materials at a beginning level for novice subjects participating in this study, based on the NIST guidelines (NIST SP 800-50, 2003).

3.5. Post-test assessment

Students needed to answer 20 multiple-choice questions related to their security awareness levels in perception and comprehension. To adequately assess the learning performance of users at the projection level, subjects need to first decide on e-mail titles that might cause future damage to their systems. Following their choice of suspicious e-mails were explanations in the short-essay format for potential damages and actions to be taken.

3.6. Experimental system

To meet the unique needs of our experiments, we adopted XOOPS, an extensible and object oriented dynamic web content management system written in PHP, to develop our experimental system (http://www.xoops.com). We developed two learning modules to record learning behavior of students. The first learning module enabled us to record the time duration that users spent in reading course materials. This module also recorded the frequency that users clicked on the course materials. The second module assisted us in estimating the ability of users to project potential security risks.

4. Data analysis

We ran statistical analyses of the collected data using SPSS for Windows 13.0. We first ran a regression analysis to assess the degree of correlations among three security awareness levels: perception, comprehension and projection. The results are presented in Table 1. Analysis of the results showed that a high reliability of correlation existed among the three security awareness levels. First, the ability to comprehend security risks was significantly correlated with the ability to project potential risks. The standardized coefficient was 0.795. This indicates that 79.5% of variance in the ability of a user to project future risks can be explained by the ability of a user to comprehend security risks. Second, the correlation between the ability to perceive risks and the ability to project potential risks was also positively correlated, with the coefficient as 0.569. This indicates that the ability of users to perceive risks could explain 56.9% of the variance. Third, the correlation coefficient between the ability to perceive and comprehend security risks was 0.539. This indicates that the ability of users to perceive risks can explain 53.9% of the variance.

Table 1
Regression analysis in awareness levels

Model	*F*	*p*-Value	Standardized coefficients
Comprehension * projection	259.456	0.000(a)	0.795
Perception * projection	72.273	0.000(a)	0.569
Perception * comprehension	61.955	0.000(a)	0.539

Table 2
Model 1 analysis result

Model	Variable	Standardized coefficients	*T*	*p*-Value	R^2
1	Perception	0.198	3.494	0.001	0.66
	Comprehension	0.688	12.173	0.000	

Dependent variable: projection.

Table 3
Model 2 analysis result

Model	Variable	Standardized coefficients	*T*	*p*-Value	R^2
2	Perception	0.539	7.871	0.000	0.29

Dependent variable: comprehension.

Since all three constructs are correlated with each other, it was important to identify their causal order and determine the significance of predictive power of one construct for another construct. Hence, we ran two path analyses of the causal relationships among these three constructs. Table 2 shows the path analysis result of the predictive power of perception and comprehension for the dependent variable of projection ability. Table 3 shows the path analysis result of the predictive power of comprehension for projection. As shown in the regression analysis, their relationships continued to exist. However, a closer examination showed that improvement in the ability of users to perceive and comprehend risks together could largely enhance their ability to project security risks (R^2 increased from 0.29 to 0.66). It is apparent that although the improvement in comprehension enhanced the ability of users to project potential risks, this construct alone was insufficient. The ultimate goal of a SA program is to improve not only the perception, but also the comprehension ability of users. Achieving this goal can result in substantial improvement in the ability of users to project potential information security risks. Thus, Hypotheses H1 and H2 are statistically supported (see Fig. 2).

We ran a series of *t*-tests to investigate if users of this study receiving different treatments that vary in the degree of media richness can have varying learning performance. Table 4 shows the comparative mean post-test scores between the groups of users receiving the hypertext and the multimedia treatments. The group of users receiving the hypertext-based security awareness training (mean = 13.31) outperformed the group of users receiving multimedia-based training (mean = 12.16). Hypothesis H6 proposed otherwise; therefore, H6 was rejected in Experiment I. On the other hand, Hypotheses H7 and H8 are supported. In the post-test of the comprehension competency, the group of users receiving multimedia-based security awareness training (mean = 12.51) outperformed the group of users receiving hypertext-based training (mean = 11.22). The former group (mean = 12.85) also scored higher than the latter group (mean = 10.45) in the performance of projecting security risks. Hence, Hypotheses H7 and H8 are supported.

We ran another *t*-test to compare the mean scores between the groups of users receiving multimedia-based and hypermedia-based security awareness training approaches. We hypothesized that hypermedia is a more rich media than multimedia. Thus, it is plausible that hypermedia-based security awareness training can be more effective than multimedia-based training. Table 5 shows the initial analysis of

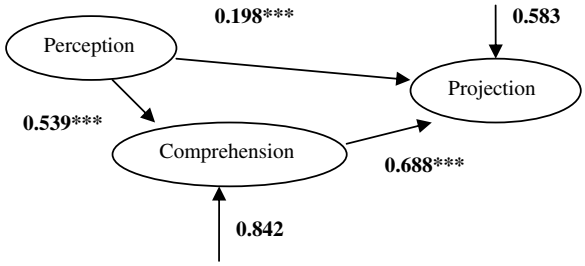

Fig. 2. Path analysis result.

Table 4
t-Test in Experiment I

Group	*N*	Mean	SD	*F*	*t*	*p*-Value
Perception						
Hypertext	51	13.31	2.267	0.047	2.613	0.010
Multimedia	51	12.16	2.203			
Comprehension						
Hypertext	51	11.22	2.335	0.994	−2.683	0.009
Multimedia	51	12.51	2.533			
Projection						
Hypertext	51	10.45	2.403	3.796	−5.645	0.000
Multimedia	51	12.85	1.867			

Table 5
t-Test in Experiment II

Group	*N*	Mean	SD	*F*	*t*	*p*-Value
Perception						
Multimedia	51	12.16	2.203	0.243	−0.607	0.545
Hypermedia	51	12.43	2.36			
Comprehension						
Multimedia	51	12.51	2.533	1.114	−0.183	0.855
Hypermedia	51	12.61	2.857			
Projection						
Multimedia	51	12.85	1.867	1.283	−0.188	0.851
Hypermedia	51	12.93	2.298			

Table 6
t-Test in adjusted Experiment II

Group	*N*	Mean	SD	*F*	*t*	*p*-Value
Perception						
Multimedia	51	12.16	2.203	0.187	−3.019	0.004
Hypermedia	23	13.87	2.38			
Comprehension						
Multimedia	51	11.84	2.185	0.166	−4.742	0.000
Hypermedia	23	14.48	2.274			
Projection						
Multimedia	51	12.85	1.867	1.346	−2.761	0.007
Hypermedia	23	14.21	2.131			

Table 7
Results of hypotheses testing

	Hypotheses	Results
H1	*Hypotheses 1*: Users with higher perceived security risks are more likely to have higher comprehension of these risks	Support
H2	*Hypotheses 2*: Users with higher comprehension of security risks are more likely to have a better ability to project potential security risks	Support
H3	*Hypothesis 3*: Hypermedia-based online SA programs are more effective than multimedia-based ones in enhancing the perception of users about security awareness	Support
H4	*Hypothesis 4*: Hypermedia-based online SA programs are more effective than multimedia-based ones in enhancing the comprehension of users about security awareness	Support
H5	*Hypothesis 5*: Hypermedia-based online SA programs are more effective than multimedia-based ones in enhancing the projection ability of users about security awareness	Support
H6	*Hypothesis 6*: Multimedia-based online SA programs are more effective than hypertext-based ones in enhancing the perception of users about security awareness	Reject
H7	*Hypothesis 7*: Multimedia-based online SA programs are more effective than hypertext-based ones in enhancing the comprehension of users about security awareness	Support
H8	*Hypothesis 8*: Multimedia-based online SA programs are more effective than hypertext-based ones in enhancing the projection ability of users about security awareness	Support

the 51 subjects in each group receiving either training approach. The analysis results did not support our hypotheses that the difference of learning performance exists between these two groups in three security awareness tasks: perception, comprehension and projection.

A closer investigation of the usage behavior, based on the logs of information recorded by our developed learning systems, shows that not every participant spent time on or clicked the hyperlinks. We therefore excluded these participants from the population and ran another *t*-test. This new *t*-test is shown in Table 6. The adjusted group of users receiving hypermedia-based training outperformed those receiving multimedia training in all security awareness tasks. In the post-test of perception competency, the group of users receiving hypermedia-based security awareness training (mean = 13.87) outperformed the group of users receiving multimedia-based training (mean = 12.16). Hypothesis H3 is supported. In the post-test of comprehension competency, the group of users receiving hypermedia-based security awareness training (mean = 14.48) outperformed the group of users receiving hypertext-based training (mean = 11.84). Hypothesis H4 is supported. The former group (mean = 14.21) also scored higher than the latter group (mean = 12.58) in the performance of projecting security risks. Hypothesis H5 is supported. Hence, Hypotheses H3, H4 and H5 are supported. Table 7 summarizes the testing results of these eight hypotheses.

5. Discussions and implications

Human errors have been a significant source of information security risks over the decades (Im & Baskerville, 2005). It is imperative to minimize human errors in order to improve organizational security awareness. An increasing number of users can access SA programs if they are delivered online synchronously or asynchronously. The chance of committing human errors can be lowered as the base of users

who are more aware of security risks is expanded. The culture of information security awareness can be fostered and instilled in an organization (Carblanc & Moers, 2003). Hence, the organization can be much more secure from internal and external security threats with a heightened SA program.

The perception, comprehension and projection of information security risks by users are three critical prerequisites to improved security awareness levels (Endsley, 1995). The ordered sequence of effects exists among these three elements. An improved perception can enhance comprehension, thereby advancing the ability of users to project information security risks. Although the improvement of perception can bypass the factor of comprehension, and directly help improve the ability of users to project information security risks, the strength of this effect is not as strong as that of the joint effects of perception and comprehension on the improvement of projection ability. A study asserts that the gap between the perceptions and comprehension of municipal security analysts and auditors concerning the auditor's report exists (Gaffney & Lynn, 1989). Therefore, an effective online SA program needs to target at improving these two abilities.

Online media differ in the element of media richness. The influence of media richness on the improvement of the perception, comprehension and projection of information security risks by users are too strong to be underestimated. Our experiment discovered that users receiving hypermedia-based security awareness training outperformed those receiving multimedia-based training in the tasks of security perception, comprehension and projection. Also due to the influence of media richness, users receiving multimedia-based training outperformed hypertext-based training in comprehension and projection tasks.

Our findings indicate that hypertext-based training is more effective than multimedia-based training in enhancing users' perceptions of security risks. This finding contradicts our hypothesis that the media richness has a strong positive influence on the enhancement of SA in the perception task. Cognitive load theory suggests that a person has a limited processing capacity in his/her working memory (Miller, 1956). Ineffective allocation of the limited capacity can result in the learning ineffectiveness (Sweller, 1999). Multimedia-based instruction that incorporates visual, audio and video data formats is more likely to impose an excessive working memory load (Najjar, 1996; Tergan, 1997). As such, multimedia-based instruction is not necessarily effective for all kinds of learning tasks. Sometimes, the instruction can create negative effects because it can divert the attention of learners from the studied subjects (Kalyuga, Chandler, & Sweller, 2000). Perceived security risks are a prerequisite to the improvement of comprehension and projection. This task has the least complexity in comparison. Multimedia-based instruction may detract learners from the studied subjects. Therefore, instructors of an online SA program should discourage the use of rich media if all they want to do is promote an effective learning of tasks in the area of perception. However, when users attempt to advance their security awareness level from the perception to comprehension and projection, the importance of media richness is increased substantially. Our study shows that multimedia-based instruction outperforms hypertext-based instructions in the tasks of comprehension and projection. Multimedia-based instructions can help cope with the inter-group communication problems and support social relationships (Fish, Kraut, Root, &Rice, 1993). When users are asked to comprehend and project potential security risks, situations are ambiguous or unclear. Users have preferences for higher rich media when the ambiguity of situations is high. These advantages may result in the salient effect of multimedia-based instruction on improving security awareness levels.

Hypermedia-based instruction incorporates the dimensions of adaptability and interactivity in addition to the advantages of media richness. If properly used, hypermedia can manipulate objects and relations between spaces and locations in flexible modes (e.g. story telling, gaming, 3D, virtual reality) (Romero, Santiago, & Correia, 2004). Hypermedia helps organize objects (e.g. multimedia, text, picture and audio) and connects them via hyperlinks. The distinct differences between hypermedia and multimedia ease the navigation and retrieval process, which can promote the effectiveness of decision-making (Huang, 2003). Because of these advantageous effects, hypermedia-based instructions outperform multimedia-based instructions in all tasks of security awareness training: perception, comprehension and projection.

6. Conclusions

Enhancing security awareness levels of general users in the tasks of perception, comprehension and projection has been a major concern in the growing interconnected, society. Despite the adoption of SA programs, many organizations are still vulnerable, especially to human-side security threats. Online media incorporate many pedagogical merits, such as interactivity, adaptability, social learning, convenience, and instant feedback. This experimental study investigates if online media with high media richness would be more effective that those with low media richness to enhance the progress of learning from the perception to comprehension and then to projection of security risks. The results of this study confirm the existence of positive correlations between the degree of media richness and the improvement of security awareness levels. However, an exception of these findings noted in this study is the potential negative effect of too much media richness on learning performance. Perhaps organizations that plan to implement an online SA program need to aware of this potential negative effect. Future research may want to repeat this experiment by enlarging the difference (effect size) in media richness among media. This kind of research can help clarify the online confounding effect identified in this study.

The second finding discovered in this research is the cause-and-effect among perception, comprehension and projection. Although improvement of perception and comprehension can both advance a user's ability in the task of projection, comprehension has a higher predictive power than perception for the difference in projection. An organization needs to roll out a series of online SA programs oriented toward perception, comprehension, and projection.

The third finding noted in this research is that hypermedia-based instruction is the most effective approach to enhance SA levels, followed by multimedia-based, and then hypertext-based instruction. Hypermedia-based instruction combines features of both hypertext- and multimedia-based instruction, and also includes interactivity and adaptability. These advantageous features make hypermedia-based the most attractive approach to deliver online SA programs. An organization needs to invite pedagogical, security and web-design experts to integrate those features into an online SA program.

References

Anderson, J. R. (1983). *The architecture of cognition*. Cambridge, MA: Harvard University Press.

Bruner, J. (1966). *Toward a Theory of Instruction*. Cambridge, MA: Harvard University Press.

Carblanc, A., & Moers, S. (2003). *Towards a Culture of Online Security*. Paris: Organisation for Economic Cooperation and Development. p. 30.

Claburn, T. (2005). Machine wars: The battle between good and evil in cyberspace is increasingly fought with automated tools. Information Week, January 17, pp. 54–63.
Daft, F. L., & Lengel, R. H. (Eds.). (1984). *Information richness: A new approach to manager information processing and organization design*. Greenwich, Connecticut: JAI Press.
Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors Journal, 37*(1), 32–64.
Endsley, M. R., & Garland, D. J. (Eds.). (2000). *Theoretical underpinnings of situation awareness: A critical review. Situational analysis awareness and measurement*. Mahwah, NJ: Lawrence Erlbrum Associates.
Eppler, M. J. (2006). A comparison between concept maps, mind, maps conceptual diagrams, and visual metaphors as complementary tools for knowledge construction and sharing. *Information Visualization, 5*(3), 202.
Fish, R. S. , Kraut, R. E. , Root, R. W. , & Rice, R. E. (1993). Video as a technology for informal communication. Communications of the ACM, New York, *36*(1), 48.
Gaffney, M. A., & Lynn, S. A. (1989). The expectations gap and municipal auditing. *The Government Accountants Journal, 38*(2), 17.
Highland, H. J. (1995). Security awareness and the persuasion of managers. *Computers & Security, 14*(1), 27.
Huang, L. (2003). Ten pointers for enhancing learners' motivation. Business Communication Quarterly, New York, *66*(4), 88–95.
Im, J. J., & L Baskerville, R. (2005). A longitudinal study of information system threat categories: the enduring problem of human error. *Database for Advances in Information Systems, 36*(4), 68–79.
Johnston, J., Eloff, J. H. P., & Labuschagne, L. (2003). Security and human computer interfaces. *Computers & Security, 22*(8), 675–684.
Jones, D. G., & Endsley, M. R. (1996). Reducing situation awareness errors in aviation. *Aviation, Space and Environmental Medicine, 67*(6), 507–512.
Kalyuga, S., Chandler, P., & Sweller, J. (2000). Incorporating learner experience into the design of multimedia instruction. *Journal of Educational Psychology*(92), 126–136.
Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289–296.
Lawrence, A. , Gordon, L. A. , Loeb, M. P. , Lucyshyn, W. , & Richardson, R. (2006). CSI/FBI Computer Crime and Security Survey. 2006: Computer Security Institute.
Leach, J. (2003). Improving user security behaviour. *Computers & Security, 22*(8), 685–692.
Miller, G. A. (1956). The magical number seven, plus or minus two: some limits on our capacity for processing information. *Psychological Review*(63), 81–97.
Najjar, L. (1996). Multimedia information and learning. *Journal of Educational Multimedia and Hypermedia*(5), 129–150.
NIST SP 800-50 (2003). National Institute of Standards and Technology (NIST). Building aninformation technology security awareness and training program (NIST SP 800-50). Washington, DC: US Department of Commerce.
NIST SP 800-16 (1998). National Institute of Standards and Technology (NIST) information technology training requirements: A role- and performance-based model (NIST Special Publication 800-16). Washington, DC: US Department of Commerce.
Nielsen, J. (2000). Hard-to-use sites will fail. The Irish Times, January 2000.
Novak, J. D. (1990). Concept maps and Vee diagrams: Two metacognitive tools for science and mathematics education. *Instructional Science*(19), 29–52.
Power, R., & Forte, D. (2006). Case study: A bold new approach to awareness and education, and how it met an ignoble fate. *Computer Fraud & Security* (5), 7–10.
Romero, L., Santiago, J., & Correia, N. (2004). Contextual information access and storytelling in mixed reality using hypermedia. *Computers in Entertainment, New York, 2*(3).
Schlienger, T., & Teufel, S. (2003). Information security culture – From analysis to change. In *3rd annual information security South Africa conference, 9–11 July 2003, information security South Africa – Proceedings of ISSA 2003, Johannesburg, South Africa*.
Schneider, E. C., & Therkalsen, G. W. (1990). How secure are your system? Avenues to Automation, November 1990, pp. 68–72.
Sweller, J. (1999). *Instructional design*. Melbourne: ACER.
Tergan, S. (1997). Misleading theoretical assumptions in hypertext/hypermedia research. *Journal of Educational Multimedia and Hypermedia*(6), 257–283.
Valentine, J. A. (2006). Enhancing the employee security awareness model. *Computer Fraud & Security*(6), 17–19.
Wilson, M., & Hash, J. (2003). *Build awareness and training program*. National Institute of Standards and Technology (NIST).
Wireless News "Cisco Study: Despite Claiming Security Awareness, Many Remote Workers Engage in Risky Online Behavior" (2006). Wireless News, October 10, p. 1.