Contents lists available at ScienceDirect

Computers & Education

journal homepage: www.elsevier.com/locate/compedu

The impact of information richness on information security awareness training effectiveness

R.S. Shaw [a], Charlie C. Chen [b], Albert L. Harris [b,*], Hui-Jou Huang [c]

[a] *Department of Information Management, Tamkang University, Taipei, Taiwan*
[b] *Appalachian State University, Department of Computer Information Systems, Boone, NC 28608, United States*
[c] *HTC Corporation, Taipei, Taiwan*

ARTICLE INFO

Article history:
Received 13 February 2008
Received in revised form 26 June 2008
Accepted 27 June 2008

Keywords:
Information richness
Information security
Security awareness
Hypermedia
Multimedia
Hypertext

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.

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.

* Corresponding author. Tel.: +1 828 262 6180; fax: +1 828 262 6190.
E-mail address: harrisal@appstate.edu (A.L. Harris).

0360-1315/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compedu.2008.06.011

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).