Forget the Fluff: Examining How Media Richness Influences the Impact of Information Security Training on Secure Behavior

Jeffrey L. Jenkins
The University of Arizona
jjenkins@cmi.arizona.edu

Alexandra Durcikova
The University of Arizona
alex@eller.arizona.edu

Mary B. Burns
The University of Arizona
mburns@cmi.arizona.edu

Abstract

User-initiated security breaches are common and can be very costly to organizations. Information security training can be used as an effective tool to improve users' secure behavior and thus alleviate security breaches. Via the lens of learning, media richness, and cognitive load theories, this research examines how to improve the effectiveness of security training. We conduct a realistic laboratory experiment to examine the influence of training with different degrees of media richness on secure behavior. We found that training with lean media richness improved secure behavior more than training with highly-rich media. Suggestions for researchers and practitioners are provided.

1. Introduction

The news is full of headlines of information security breaches [18], and most security compromises and exploits are a result of employees' insecure behavior [37, 11, 1]. Indeed, the human is often referred to as the weakest link of security [5], and human-caused security breaches can be very costly to organizations [16]. Thus, an important area of research is to explain how to improve users' secure behavior, defined as users' compliance with their organization's security policy [22].

Information security training (hereafter referred to as training) has been shown to improve secure behavior [e.g., 34, 22]. Research has just begun to discover how to design training programs to maximize their influence on secure behavior [e.g., 34]. In our research, we examine how media richness influences the effectiveness of training to improve secure behavior. Different media can be used to implement training; however, it is not clear how effective these different approaches are. Media richness theory suggests that managers should make rational choices matching a particular communication medium to a specific objective and to the degree of richness required by that objective [40]. This study examines the effectiveness of highly-rich media versus lean media training focused on *how* to be secure. In summary, we address the following research question: *How does media richness in training materials influence secure behavior?*

2. Theory development

In this section, we utilize *learning theory* to summarize relevant literature and explain how training can alleviate security vulnerabilities. We then utilize *media richness theory* and *cognitive load theory* to explain how media richness influences the effectiveness of training on secure behavior.

Users who receive training should demonstrate higher secure behavior than users who do not receive training [22, 34]. Several theoretical perspectives, collectively known as *learning theory*, have been adopted to explain why training on how to behave securely influences secure behavior [20]. Generally, these perspectives can be summarized into three schools of thought—behaviorism, cognitivism and constructivism [14]. We briefly explain each perspective for the purpose of providing both a taxonomy of security training literature and justification that training improves secure behavior.

Behaviorism [36] posits that learning is manifested by changes in behavior caused by the environment. In our context, the environment refers to the training measures undertaken by an organization. Because behaviorism treats the mind as a "black box", learning is accomplished by providing reinforcement, or rewards and punishment. When a training program rewards secure behavior, users will behave securely in the future; when a training program punishes insecure behavior, users will avoid that behavior in the future. For example, Straub and Welke [37] found that communicating the certainty and severity of punishment can influence IS secure behavior. Goodhue

978-0-7695-4525-7/12 $26.00 © 2012 IEEE
DOI 10.1109/HICSS.2012.285

and Straub [17] examined how security concerns influence secure behavior. Reinforcement is most relevant when it is concurrent with the targeted behavior.

Cognitivism [33, 32] looks beyond behavior to explain mental-process learning. Cognitivism posits that the brain is an active organized processor of information. Training influences secure behavior by being received through the senses, processed by short term memory, and then stored in long-term memory [30]. Importantly, information must capture users' attention and be organized into a meaningful schema for learning to be accomplished [29, 30]. In the information security field, cognitivism researchers have attempted to find factors that influence attention and memorability. For example, Puhakainen and Siponen [34] found that factors such as repetition and personal relevance improve the effectiveness of training.

Finally, constructivism [3] posits that users construct new ideas and concepts based on how they interpret past experiences. In other words, users create their own knowledge and reality from their own experiences. According to a constructivism view, security training influences secure behavior by providing a mechanism for users to experience security issues (e.g., mock security breaches), which leads them to form their own thoughts and knowledge regarding how to be secure and why it is important to be secure. Although constructivism has not been applied extensively to creating information security training programs, it has been applied in information systems to help users understand the Internet [6] and build job skills [4]. In summary, we concur with learning theory perspectives (behaviorism, cognitivism and constructivism) that training should influence secure behavior.

H1. Users who receive training will exhibit higher secure behavior than users who receive no training.

A key characteristic of training programs that can influence security-related outcomes is the degree of media richness. Media richness theory [10] describes that communication media vary by the degree they are able to reproduce information. Richness refers to the number of cues that a media can communicate (e.g., visual, audio, interaction) to reproduce information. The richest communication medium is face-to-face communication; less-rich (lean) communication media includes only text or only audio. Media richness theory argues that richness is determined by objective characteristics of the media, although subsequent theories have argued that processing media characteristics is not objective [15, 7, 42]. According to media richness theory, there has to be a fit between the richness of the media and the objective [40], e.g. messages about compliance with secure behavior.

Previous research has found mixed results regarding the influence of training media richness on the perception, comprehension, and projection of security awareness [35]. Namely, research has found that hypermedia-based (highly-rich media) online security awareness programs is always more effective than multimedia-based ones (medium-rich media) in influencing perception, comprehension, and projection of security awareness. Multimedia-based (medium-rich media) online security awareness programs are more effective than hypertext-based ones (lean media) in influencing comprehension and projection of security awareness, but surprisingly is less effective when predicting perceptions of security awareness. The authors suggest that this difference may be due to an increase in cognitive load caused by rich media [35]. We build on this research to explain and empirically test how media richness of training influences not only perceptions of but also actual secure behavior. Because we concur that media richness may result in an increase in cognitive load, we build on cognitive load theory (CLT) to explain the relationship among media richness, training and secure behavior. CLT, originating from cognitive psychology, explains the inherent limitations of concurrent working memory load [38]. Humans are limited in the amount of information they can hold in their working memory and the number of operations they can perform on this information. Stimuli compete for the users' attention and, thus, for users' limited working memory and processing ability [26]. Rich media offer several channels of information that compete for attention and working memory. Based on CLT, we propose that security training media with a high degree of media richness may communicate information that distracts from the core message of how to be secure. For example, although a rich online training video may explain in detail how to behave securely, the user may be distracted by indirect messages such as the voice, attire of the narrator, special effects, graphics, etc. This information communicated via other channels may successfully obtain users' attention and increase their cognitive loads. By doing so, the user has less working memory to devote to learning how to be secure. In summary, we propose:

H2. Users who receive training from highly-rich media will exhibit lower secure behavior than users who receive training from lean media.

3. Experimental design

To help test our hypotheses, we deployed a single-factor experiment with three levels—1) no training (baseline group), 2) training with lean media and 3) training with highly-rich media. A total of 238 individuals participated in the experiment. Students, who composed 98.5% of the total sample, were chosen as the population because they are an accurate representation of new employees integrating into a new organization [19], and will be the audience of new-employee security training programs in the near future. The average years of education for the participants was 3.2, indicating that the students would soon be entering the workforce. Thus, the results of this study may be generalized to junior employees and can influence new employee orientation programs.

Sixty-percent of the participants were male and the average age was 23.1. The five most represented disciplines for the participants' majors were MIS (37%), Business Management (18%), Marketing (11%), Accounting (9%), and Finance (6%). Seventy percent of the participants were American, 8% Chinese, 6% Mexican, 4% Indian, and 12% other.

3.1. Experimental task and manipulations

An experiment was designed to provide a training treatment with different levels of media richness to participants and then monitor the participants' secure behavior as they completed a task in a realistic corporate computer setting. To mimic a realistic corporate situation that a new employee would experience, participants were told that they had been employed by a corporation, and that their first task was to complete a financial report on a corporate Windows workstation that required them to use three different sources of information (e-mail, corporate wiki, and a document repository). Each participant was given an orientation packet including a welcome letter from the CEO, a series of corporate policies including the password policy, and a username to access a corporate workstation. The orientation packet included all information necessary for participants to complete their task. The task required participants to interact with several different electronic information sources (e.g., wiki, document repository) that each required a log-in.

To replicate better a realistic corporate environment, we controlled for whether users had single sign-on or multiple sign-on functionality. While some organizations are moving to single sign-on, many still use multiple sign-on that is more cognitively demanding. Approximately half of the participants were randomly provided single sign-on functionality in each of the three treatment groups, which allowed them to access all electronic information sources with a single user name and password. The other half of the participants was required to create a username and password for each electronic information source (multiple sign-on). During the experiment, we captured users' passwords and stored them in a secure database. The passwords were analyzed after the experiment. After finishing their task, participants were asked to complete a questionnaire.

As participants arrived at the experiment, they were required to participate in a) no training, b) lean media training or c) highly-rich media training. The content of the training (and also the security policy document given to every subject) was adopted from the SANS Institute (http://www.sans.org/) – a recognized information security institution responsible for several standards in the information security world. The training treatments were manipulated per the four objective attributes of media richness suggested by Daft and Lengel [9]—1) the media'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.

Sample screenshots of the lean media training are shown in Figure 1. The lean media training video was a narrated PowerPoint slide presentation and the duration was approximately 5 minutes long. The lean media training 1) did not provide immediate feedback, 2) had only two channels of communication available (written text and narration), 3) had little language variety (only read the security policy), and 4) focused little on the recipient.

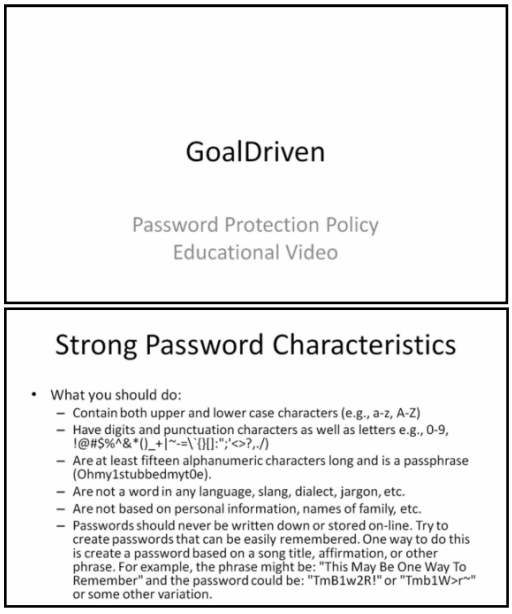

Figure 1. Lean media training treatment

The highly-rich media treatment was also approximately five minutes long. To increase media

richness, the program 1) provided more feedback and explanation of security practices, 2) gave users more channels and cues to evaluate (e.g., narrated by a person that participants could see and hear; text; and images), 3) provided more language variety with additional explanation and guidance, and 4) intent was focused on the recipient by making the video relevant to the scenario and the individual by ingratiation and more context-specific detail about participants' new role as new employees of the fictitious company. Example screenshots from the highly-rich media treatment are shown in Figure 2.

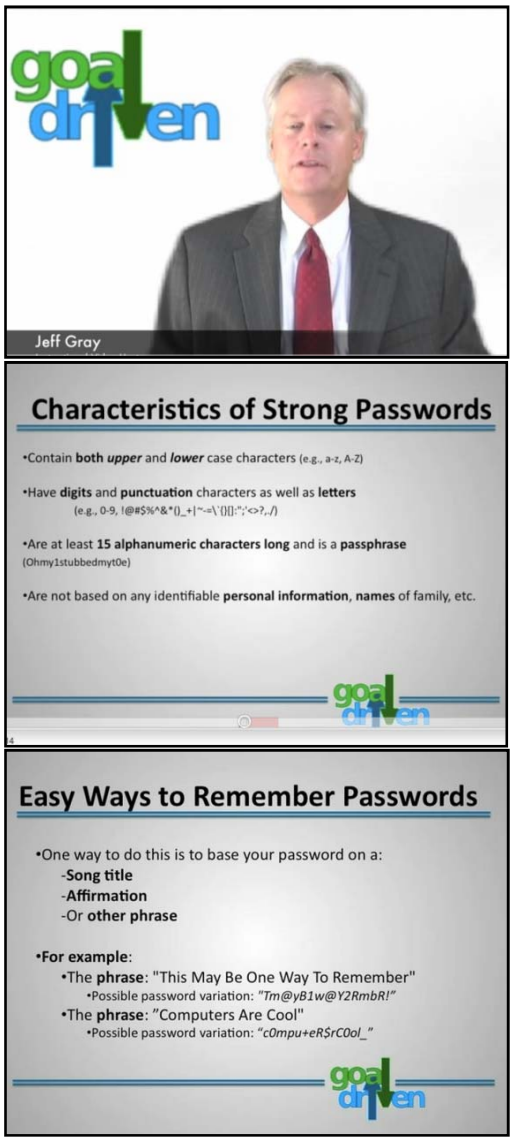

Figure 2. Highly-rich training treatment

3.2. Independent and dependent variables

3.2.1. Independent variables. The type of security training (no training, lean training, and highly-rich training) represents levels of our independent variable. In the post-treatment questionnaire, several potentially confounding variables identified in previous studies as predictors of secure behavior were also collected and controlled for, including computer self-efficacy [13, 39, 31], perceived ease of use [13, 12], perceived cognitive effort [24, 41], security policy satisfaction [2], single vs. multiple sign-on [22], and age.

3.2.2. Dependent variables. The measure for Secure Behavior was calculated objectively as a degree of compliance with the security policy limited to password creation. Thus, the results of our study are also limited to this scope. Password policies, although not the only type of secure behavior, are nevertheless ubiquitous because employees are often required to create passwords not only within the organization but also with external entities that do not implement strict password checks. During the experiment, participants' passwords for all electronic information sources were securely stored as plaintext in Microsoft Active Directory. Passwords were analyzed using a custom script developed according to the security policy criteria adopted from the SANS Institute. Figure 3 displays the algorithm that was used to generate a score based on the password criteria that is outlined in the password policy. Since the password compliance score ranged between 0 – 4, the percentage compliance was calculated by dividing the score by 4. We also collected information regarding participants' perceptions of training adequacy using a scale adapted from D'Arcy et al. [8].

$$\text{Password Score} = R + \frac{\sum_{k=0}^{n} \frac{\text{L}}{15} + \text{D} + \frac{\text{U} + \text{L} + \text{D} + \text{P}}{4}}{n}$$

N = number of passwords
R = 1 if password was unique, 2 if password was not unique
L = password length (SANS suggest at least 15 characters)
D = password found in dictionary (1 = no, 0 = yes)
Password Complicity:

- U = contains uppercase letter(s) (1 = yes, 0 = no)
- L = contains lower case letter(s) (1 = yes, 0 = no)
- D = contains digits (1 = yes, 0 = no)
- P = contains punctuation / special characters (1 = yes, 0 = no)

Figure 3. Calculation of secure behavior

3.3. Data analysis and results

Convergent and discriminant validity and reliability of all measurement scales were verified

through a confirmatory factor analysis as well as construct correlations and cross-correlations (Table 1). A manipulation check using ANOVA confirmed that subjects distinguished media richness between the lean media training and highly-rich media training (df=2, f=10.238, $p < 0.001$).

ANOVA was then performed to test for a difference in secure behavior means among the three treatment groups. A significant difference was present (df = 2, f=20.760, $p < 0.001$). A Bonferroni comparison of means showed that participants who received the lean media training treatment displayed significantly higher secure behavior than participants in the control group (MD = 0.536 SE = 0.084; $p < 0.001$) and the participants who received the highly-rich media training treatment (MD = 0.425 SE = 0.11; $p < 0.001$). Participants who received the highly-rich media training treatment did not exhibit higher secure behavior than no training treatment (MD = 0.111 SE = 0.104; p = 0.854). The means for secure behavior for each treatment group are displayed in Figure 4.

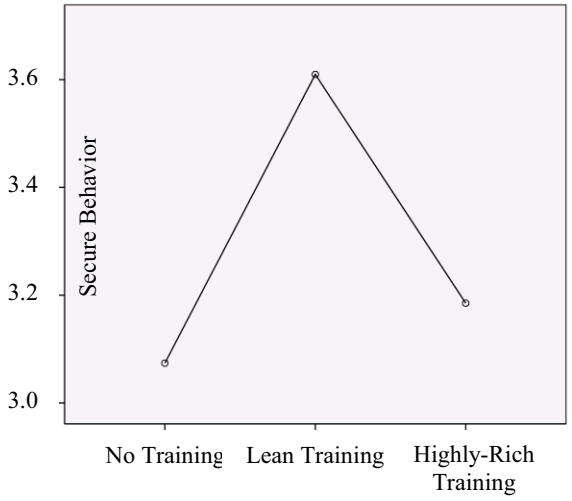

Figure 4. Secure behavior means for each treatment

As a supplemental analysis, we conducted an ANOVA comparing the means of participants' perceptions of training adequacy (Figure 5). Perceptions of training adequacy for participants who received the lean media training treatment were significantly higher than the perceptions of training adequacy for participants in the no training group (MD = 1.78 SE = 0.226; $p < 0.001$) and the perceptions of training adequacy for participants who received the highly-rich media training treatment (MD = 0.783 SE = 0.296; p = 0.026). Participants who received the highly-rich media training treatment also had significantly higher perceptions of training adequacy than the control group (MD = 0.999 SE = 0.278; p = 0.001).

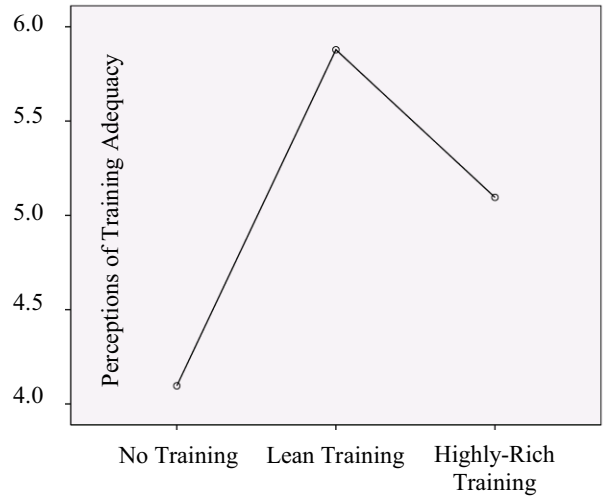

Figure 5. Perceptions of adequacy of training means for each treatment

We then conducted an ANCOVA analysis using a General Linear Model to consider the influence of our manipulations along with the control variables we identified. Table 2 displays the results of the ANOCOVA analysis, and Table 3 displays the parameter estimates. Both training (df=2, f=25.012, p <.001) and single sign-on (df=1, f=51.878, p <.001) influenced secure behavior. Consistent with the ANOVA, lean media training had a significant parameter estimate of .419 (approximately a 10.5% increase in secure behavior). However, the highly-rich media training did not have a significant parameter estimate. The significant parameter estimate for single sign-on was .535 (approximately a 13.4% increase in secure behavior).

4. Discussion

The goal of this research was to answer the following question "*How does media richness in training materials influence secure behavior?"* First, we hypothesized that users who receive training will exhibit higher secure behavior than users who receive no training. This hypothesis was partially supported. Lean media training resulted in significantly higher secure behavior than no training. However, training from highly-rich media did not result in a significantly higher degree of secure behavior than no training.

Second, we hypothesized that users who receive training from a highly-rich media source will exhibit lower secure behavior than users who receive training from a lean media source. This hypothesis was

supported. Furthermore, a post-hoc analysis revealed that users perceived highly-rich media training as even less adequate than lean media training.

4.1. Implications for research

Past research has shown that media richness normally improves perception, comprehension, and projection of security awareness, except when comparing multimedia-based (medium-media richness) training with hypertext-based ones (low media richness) [35]. We expand this study in the context of training programs that teach users how to behave securely and then measuring actual secure behavior in terms of compliance with the password policy. Our results support that highly-rich media may be problematic in security training and awareness programs, especially when the training introduces concepts that require high cognitive attention from the subject. In this case, lean media is a better fit because it does not overly tax the user whose cognitive load is already strained due to the nature of the message. Hence, our theoretical explanation of why media richness may impede secure behavior based on cognitive load theory is very useful in the area of security training. Specifically, channels and cues compete for cognitive attention and cues not directly related to the objective (e.g., how to be secure), expend users' working memory, and deter users from focusing on the training objective. The newly prescribed secure behavior requires a user to switch cognitive gears from an automatic mode to a conscious mode [25] to integrate the new security policy into their everyday lives. Future research should investigate how and when this shift to active thinking happens.

Second, drawing on learning theory, our research provides a possible taxonomy of security training literature. Security training can be categorized in three gestalt categories – behaviorism, cognitivism and constructivism. It is important to note that a security training program can take a multi-method approach and fit into more than one category. This taxonomy for research is beneficial because it can help organize and identify gaps in security training literature. Future research can examine which approach or combination of approaches is the most effective with respect to security training.

Finally, training in this study was given the day of the experiment. Future research should examine the longitudinal effect of follow-up training and determine how often and at what intervals it must be repeated so that the effects of training are not lost. In addition, rather than investigating just the effects of training, the role of security cues (e.g., desktop background reminding users to logout when leaving the computer) should be studied. These cues require less cognitive load than training [21] and may augment training materials better than additional training sessions.

4.2. Implications for practice

Our research suggests that training material focusing on a cognitively taxing objective should be kept simple. Adding additional "fluff" to impress the audience, thus increase media richness, may not be beneficial when the goal of training is to explain a highly technical topic such as how to be secure. Rather, these extraneous cues may distract or overstimulate the user [27], and ultimately decrease the effectiveness of the training material. As the media richness theory suggests, effective managers need to match media richness with their objective. In the case of security training, the best fit is lean media.

Second, our research reiterates the importance of training. Simply giving an employee a welcome packet that contains policies does not ensure compliant behavior. In our study, lean media training had a huge impact on secure behavior. It improved the mean of secure behavior by .419 (approximately a 10.5% increase in secure behavior). Furthermore, the training, a narrated slide PowerPoint presentation that iterated the main points of the password policy, was not only simple and inexpensive to create but also was highly successful. Creating this type of lean media training does not require a huge budget, a great deal of training time for employees or trainers, or the use of media specialists.

4.3. Limitations and future research

This study has several limitations that can be addressed in future research. First, we recognize several limitations in our methodology. Our research is limited to primarily young and educated individuals. Future research should sample a more diverse population. Among the strengths of a laboratory experiment are control and the ability to establish causality [28], but this type of methodology may lack realism. We suggest that future research should test our hypotheses in a field study to increase realism and to examine whether our theoretical arguments still hold. This type of field experiment would also meet the requirement of a more diverse population that not only focuses on newly hired employees but also more tenured employees.

Second, our experiment utilized highly-rich and lean media training materials. Future research should also include the richest media, e.g., face-to-face training. Finally, we focused specifically on how media

richness influences training that explains *how* to behave securely. Future research should also examine how media richness influences training that explains *why* to behave securely. We suspect that the results of our study will not hold in a persuasion context because media richness can relate cues such as source credibility [23] that may improve the persuasiveness of training programs.

5. Conclusion

Security training can be used to improve users' secure behavior, which promises a decrease in the number of security breaches in organizations. Based on learning theory, media richness theory, and cognitive load theory, we examined how to improve the effectiveness of training materials. A laboratory experiment was conducted to examine the influence of media richness on the effectiveness of training. We found that lean media training improves secure behavior more than highly-rich media training. Surprisingly, the effect of highly-rich media training showed no significant difference from no security training. These results suggest that companies can implement relatively inexpensive lean security training to increase compliance with security policy over ten percent.

6. References

[1] A. Adams and M. A. Sasse, "Users are Not the Enemy: Why Users Compromise Computer Security Mechanisms and How to Take Remedial Measures", Communications of the ACM, 43 (1999), pp. 40-46.

[2] N. Au, E. W. T. Ngai and T. C. E. Cheng, "Extending the Understanding of End User Information Systems Satisfaction Formation: An Equitable Needs Fulfillment Model Approach", MIS Quarterly, 32 (2008), pp. 43.

[3] F. Bartlett, Remembering: A Study in Experimental and Social Psychology, Cambridge University Press, New York & London, 1932.

[4] F. Belanger and C. V. Slyke, "Abuse or Learning?", Communications of the ACM, 45 (2002), pp. 64.

[5] S. Boss, L. Kirsch, I. Angermeier, R. Shingler and R. Boss, "If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security", European Journal of Information Systems, 18 (2009), pp. 151-164.

[6] D. S. Brandt, "Constructivism: Teaching for Understanding of the Internet", Communications of the ACM, 40 (1997), pp. 112.

[7] J. R. Carlson and R. W. Zmud, "Channel Expansion Theory and the Experiential Nature of Media Richness Percpetions", MIS Quarterly, 42 (1999), pp. 153-170.

[8] J. D'Arcy, A. Hovav and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach", Information Systems Research, 20 (2009), pp. 79-98.

[9] R. L. Daft and R. H. Lengel, "Information Richness - A New Approach to Managerial Behavior and Organization Design", Research in Organizational Behavior, 6 (1984), pp. 191-233.

[10] R. L. Daft and R. H. Lengel, "Organizational Information Requirements, Media Richness and Structural Design", Management Science, 32 (1986), pp. 554-571.

[11] D. W. Davies and W. L. Price, Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer, Wiley, Chichester England; New York, 1989.

[12] F. D. Davis, R. P. Bagozzi and P. R. Warshaw, "User Acceptance of Computer-Technology: A Comparison of 2 Theoretical-Models", Management Science, 35 (1989), pp. 982-1003.

[13] T. Dinev and Q. Hu, "The Centrality of Awareness in the Formation of User Behavioral Intention Toward Protective Information Technologies", Journal of the Association for Information Systems, 8 (2007), pp. 386-408.

[14] P. A. Ertmer and T. J. Newby, "Behaviorism, Cognitivism, Constructivism: Comparing Critical Features from a Design Perspective", Performance Improvement Quarterly, 6 (1993), pp. 50.

[15] J. Fulk, C. W. Steinfield, J. Schmitz and J. G. Power, 529-552., "A Social Infomraiton Processing Model of Media Use in Organizations", Communication Research, 14 (1987), pp. 529-552.

[16] S. Goel and H. Shawky, "Estimating the Market Impact of Security Breach Announcements on Firm Values", Information & Management, 46 (2009), pp. 404-410.

[17] D. L. Goodhue and D. W. Straub, "Security Concerns of System Users - a Study of Perceptions of the Adequacy of Security", Information & Management, 20 (1991), pp. 13-27.

[18] Google, News Security Breaches, 2011.

[19] J. Greenburg, "The College Sophomore as a Guinea Pig: Setting the Record Straight", Academy of Management Review, 12 (1987), pp. 157-159.

[20] K. Illeris, Lifelong Learning as Mass Education, in C. Symes, ed., Working Knowledge, University of Technology, Sydney, 2000.

[21] J. L. Jenkins, A. Durcikova and M. B. Burns, Get a Cue on IS Security Training: Explaining the Difference between

Security Cues and Security Arguments in Improving Secure Behavior, International Conference on Information Systems Shanghai, China, 2011.

[22] J. L. Jenkins, A. Durcikova, G. Ross and J. F. J. Nunamaker, Encouraging Users to Behave Securely: Examining the Influence of Technical, Managerial, and Educational Controls on Users' Secure Behavior, 2011 International Conference on Information Systems, St. Louis, MO, 2010.

[23] A. C. Johnston and M. Warkentin, "The Influence of Perceived Source Credibility on End User Attitudes and Intentions to Comply with Recommended IT Actions", Journal of Organizational and End User Computing, 22 (2010), pp. 1-21.

[24] M. Keith, B. Shao and P. Steinbart, "A Behavioral Analysis of Passphrase Design and Effectiveness", Journal of the Association for Information Systems, 10 (2009), pp. 63-89.

[25] M. R. Louis and R. I. Sutton, "Switching Cognitive Gears - from Habits of Mind to Active Thinking", Human Relations, 44 (1991), pp. 55-76.

[26] N. J. Mackintosh, "A Theory of Attention: Variations in the Associability of Stimuli with Reinforcement", Psychological Review, 82 (1975), pp. 276-298.

[27] D. E. Mastro, M. S. Eastin and R. Tamborini, "Internet Search Behaviors and Mood Alterations: A Selective Exposure Approach", Media Psychology, 4 (2002), pp. 157-172.

[28] J. E. McGrath, J. Martin and R. A. Kulka, Judgment Calls in Research, SAGE Publications Inc, Beverly Hills, CA, 1982.

[29] G. A. Miller, "The magical number seven, plus or minus two: Some limits on our capacity for processing information", Psychological Review, 63 (1956), pp. 81-97.

[30] G. A. Miller, Plans and the Structure of Behavior, Holt, New York, 1960.

[31] B. Ng, A. Kankanhalli and Y. Xu, "Studying Users' Computer Security Behavior: A Health Belief Perspective", Decision Support Systems, 46 (2009), pp. 815-825.

[32] J. Piaget, The Equilibration of Cognitive Structures : The Central Problem of Intellectual Development, University of Chicago Press, Chicago, 1985.

[33] J. Piaget, Genetic Epistemology, Columbia University Press, New York,, 1970.

[34] P. Puhakainen and M. Siponen, "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study", MIS Quarterly, 34 (2010), pp. 757-778.

[35] R. S. Shaw, C. C. Chen, A. L. Harris and H. J. Huang, "The Impact of Information Richness on Information Security Awareness Training Effectiveness", Computers & Education, 52 (2009), pp. 92-100.

[36] B. F. Skinner, Science and Human Behavior, Macmillan, New York, 1953.

[37] D. W. Straub and R. J. Welke, "Coping with systems risk: Security planning models for management decision making", MIS Quarterly, 22 (1998), pp. 441-469.

[38] J. Sweller, "Cognitive Load during Problem-Solving - Effects on Learning", Cognitive Science, 12 (1988), pp. 257-285.

[39] S. Taylor and P. A. Todd, "Understanding Information Technology Usage: a Test of Competing Models", Information Systems Research, 6 (1995), pp. 144-176.

[40] L. K. Trevino, D. R. L. and R. H. Lengel, Understanding Managers' Media Choices: A Symbolic Interactionist Perspective, in J. Fulk and C. Steinfield, eds., Organizations and Communications Technology, Sage, Newbury Park, CA, 1990.

[41] W. Q. Wang and I. Benbasat, "Interactive Decision Aids for Consumer Decision Making in E-Commerce: The Influence of Perceived Strategy Restrictiveness", MIS Quarterly, 33 (2009), pp. 293-320.

[42] Y. Yoo and M. Alavi, "Media and Group Cohesion: Relative Influences on Social Presence, Task Participation, and Group Consensus", MIS Quarterly, 25 (2001), pp. 371-390.

7. Supplemental Tables

Table 1. Descriptive statistics, reliability, AVE, and inter-construct correlations

#	Construct	# of Items	Cronbach's Alpha	Internal Consistency	Mean	Std. Dev	1	2	3	4	5	6	7
1	Single Sign-On	na	na	na	0.5105	0.5009	na						
2	Training Richness	na	na	na	0.5063	0.5010	0.0124	na					
3	Secure Behavior	na	na	na	3.2699	0.6230	(0.4282)	0.3114	na				
4	Satisfaction with Policy	4	0.9649	0.9393	5.1181	1.6093	(0.1881)	0.0858	0.0998	**0.8915**			
5	Cognitive Effort	4	0.9026	0.8892	3.9462	1.6285	0.1169	(0.0781)	(0.0158)	(0.5029)	**0.8184**		
6	Ease of Use	6	0.9387	0.8901	5.2757	1.1495	(0.0382)	0.0779	0.0275	0.3781	(0.3025)	**0.7589**	
7	Computer Self-Efficacy	3	0.8827	0.8469	5.5130	1.0890	0.0370	0.0778	0.0820	0.1902	(0.1267)	0.4985	**0.8083**

SQRT(AVE) on diagonal

Table 2. General linear model tests of between-subject effects

Dependent Secure Behavior					
Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	32.757[a]	9	3.640	14.041	.000
Intercept	37.834	1	37.834	145.955	.000
Satisfaction with Policy	.008	1	.008	.029	.865
Cognitive Effort	.013	1	.013	.052	.820
Ease of Use	.392	1	.392	1.512	.220
Computer Self-Efficacy	.528	1	.528	2.035	.155
Single Sign-On*	13.448	1	13.448	51.878	.000
Training Richness*	12.967	2	6.483	25.012	.000
Single Sign-On * Training	1.410	2	.705	2.719	.068
Error	58.842	227	.259		
Total	2625.664	237			
Corrected Total	91.599	236			

a. R Squared = .358 (Adjusted R Squared = .332)

Table 3. Parameter estimates for significant variables (dependent variable - secure behavior)

Parameter	B	Std. Error	t	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Intercept	2.930	.085	34.495	.000	2.763	3.097
Single Sign-On*	.535	.066	8.062	.000	.404	.666
Highly-rich Media Training	.122	.092	-1.324	.187	-.303	.059
Lean Media Training	.419	`.098	4.282	.000	.226	.611

* Compared to the control group of Multiple Sign-On