Increasing the Persuasiveness of IT Security Communication: Effects of Fear Appeals and Self-View

BIOGRAPHIES

Heng Xu is an assistant professor of Information Sciences and Technology at the Pennsylvania State University. She received her Ph.D. degree in information systems from the National University of Singapore (2005). Her present research interests include information privacy and data security, information fusion, strategic security and privacy management, and human-computer interaction. She was a recipient of IBM PhD Fellowship (2004) and Singapore Millennium Foundation Postdoctoral Fellowship (2005). She won the Infocomm Development Authority Gold Medal and Prize (2006) for the best Ph.D. dissertation in the School of Computing at the National University of Singapore. Her dissertation on privacy considerations in the location based services was recently named as the runner up for the top dissertation in the field of information systems in 2006 ACM SIGMIS Doctoral Dissertation Award Competition.

Mary Beth Rosson is a professor of Information Sciences and Technology at the Pennsylvania State University. Her first position was at IBM's Watson Research Center, where with others in the early 1980's she contributed to the emerging field of human-computer interaction. Her research programs are in design and evaluation of interactive systems, particularly scenario-based design methods and the design and evaluation of collaborative systems for problem-solving and learning. Since moving into academia in 1994, Rosson has directed or co-directed over $6 million in grants, primarily through the Computer Science and Education directorates at NSF. Rosson is author of Usability Engineering (Morgan-Kaufmann, 2002), Instructor’s Guide to Object-Oriented Analysis and Design with Application (Benjamin Cummings, 1994), and numerous articles, book chapters, and tutorials. Rosson's recent research includes investigations of high-level programming languages and tools for end users. For example, under NSF support she is a founding member of the EUSES Consortium (www.eusesconsortium.org), an international research collaboration aimed at enhancing the quality of end user software specification and construction.

John M. Carroll is Edward Frymoyer Chair Professor of Information Sciences and Technology at the Pennsylvania State University. His research interests include methods and theory in human-computer interaction, particularly as applied to networking tools for collaborative learning and problem solving. He has written or edited 14 books, including Making Use (MIT Press, 2000), HCI in the New Millennium (Addison-Wesley, 2001), Usability Engineering (Morgan-Kaufmann, 2002, with M.B. Rosson) and HCI Models, Theories, and Frameworks (Morgan-Kaufmann, 2003). He serves on 9 editorial boards for journals, handbooks, and series; he is a member of the US National Research Council’s Committee on Human Factors and Editor-in-Chief of the ACM Transactions on Computer-Human Interactions. He received the Rigo Career Achievement Award, from ACM (SIGDOC), the Silver Core Award from IFIP, and was elected to the CHI Academy. In 2003 he received the CHI Lifetime Achievement Award from ACM.

Increasing the Persuasiveness of IT Security Communication: Effects of Fear Appeals and Self-View

Heng Xu
Penn State University
College of IST
University Park, PA 16802
1-814-867-0469
hxu@ist.psu.edu

Mary Beth Rosson
Penn State University
College of IST
University Park, PA 16802
1-814-863-2478
mrosson@ist.psu.edu

John M. Carroll
Penn State University
College of IST
University Park, PA 16802
1-814-863-2476
jcarroll@ist.psu.edu

ABSTRACT

IT security professionals strive to instill a systematic approach to security management through awareness training, procedures and policies that govern end user computing. In order to better understand end users' attitudes about performing relevant security behaviors, we have designed an experimental study to investigate the persuasiveness of security communication. More specifically, we argue that it is possible to influence security behavioral intentions of end users with fear appeal and self view manipulations made salient to them. The research program described here will suggest ways that HCI practitioners and researchers can explore the domain of security communications, and contribute to extending our theoretical understanding and practical ability to increase persuasiveness of IT security communication.

Categories and Subject Descriptors

J.4 [Social and Behavioral Sciences]: Psychology; K.4.4 [Electronic Commerce]: Security; H.1.2 [User/Machine Systems]: Human factors.

General Terms

Management, Design, Security, Human Factors.

Keywords

Information security, persuasive communication, fear appeals, self-view, policy compliance.

1. INTRODUCTION

An organization's information is among its most valuable assets and is critical to its success. The importance of information security has increased as witnessed by the increasing number of security incidents that organizations have encountered within the last few years. In the year of 2006, over 320 organizations were victims of security breaches and more than 100 million records containing sensitive personal information compromised in these security breaches [20].

To cope with increased information security threats, organizations have adopted various security measures, from technical protection means (e.g., firewall) to different information management standards (e.g., ISO 17799[1]), secure systems design methods and risk assessment techniques (e.g., OCTAVE[2]). Surprisingly, although sufficient resources are being devoted to overall security-related operating and capital expenditures, the most recent Computer Security Institute report suggests that resources devoted to end-user awareness training are less adequate than the resources devoted to either operating expenditures or capital expenditures [6]. Hence, end-user security awareness training and security computing compliance call for more attention in today's organizational security management.

The degree to which IT security professionals could align the actions of end users with the goals of organizational security management will dictate the level of success their organization has in coping with security threats [27]. In practice, a systematic approach to security management has been attempted through awareness training, procedures and policies that govern end user computing [19, 25]. Security management is an especially challenging area in that end users vary widely in level of motivations, perceptions of threat severity and computer self-efficacy [21, 29]. The decentralized computing environment in which end users exercise some degree of autonomous control over IT resources further complicates security management efforts [25].

Recently, researchers have begun to focus attention on end users' responses to security threats. Studies suggest that a combination of cognitive, social and psychological factors play a role in the formation of end user security behavioral intentions [19, 21, 25, 29]. In the research program described here, we are seeking to better understand end users' attitudes about performing relevant security behaviors. More specifically, we plan to investigate how security management might increase the persuasiveness of their communications with end users. Persuasive communication can affect end users' attitudes and motivations, and thus is a desirable aspect of security management [25]. For example, persuasive messages can be coded in security applications, or included in the

[1] ISO17799 (Code of Practice for Information Security Management) provides a common basis for developing organizational security standards and effective security management practice. http://www.iso-17799.com/

[2] OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a risk-based strategic assessment and planning technique for security. http://www.cert.org/octave/

procedure, guideline and policy documents that reflect organizational security expectations and practices.

We have designed an experimental study to investigate the persuasiveness of security communication. In this paper, we focus on two persuasion elements: fear appeals [12, 13], and self-view [23]. Both fear appeal and self-view manipulations may be manipulated to affect attitudinal change through persuasion. Thus the primary research question to be addressed in this study is: *How do fear appeals and self-view modify end user behavioral intentions associated with the recommended end user security actions?* This question will be pursued by proposing an experiment study based on theoretical foundations described below.

2. THEORETICAL BACKGROUND

2.1 Effects of Fear on Persuasion

Fear is a basic human emotion [18]. It has been defined as an internal emotional reaction composed of psychological and physiological dimensions that may be aroused when a threat is perceived [28]. Research findings regarding the impact of fear on attitudes and persuasion are equivocal. Fear was first viewed as an inhibitor to message acceptance in the seminal study conducted by Janis and Feshbach [10] which demonstrated that a communication that induced a minimal amount of fear was more effective than one that evoked a high fear response, in terms of both positive attitude change and resistance to subsequent attitudinal reversion. Confirmation of this negative relationship between fear arousal and persuasion in subsequent investigations [11, 15, 24] led practitioners to believe that fear arousal should be avoided in mass media communications. Yet, some contradictory evidence on the pattern of fear arousal and persuasion was found in other studies. For example, it was reported that fear was positively related to persuasion [26]. Specifically, highly threatening appeals are more effective than [8], or just as effective as [14, 24] less threatening messages. This suggested that fear-evoking messages should be used to increase persuasion.

To address this debate in the fear appeals literature, more and more studies have been developed to explain in an integrated manner, the conditions under which fear appeals worked and the conditions under which they failed [12, 28]. According to Keller and Block [12], when appeals arousing high levels of fear are ineffective, it is because too much elaboration on the harmful consequences interferes with processing of the recommended change in behavior. That is to say, in situations in which recipients of a message focus too much on the harmful consequences (high fear arousal), they are likely to engage defensive maneuver rather than manage the threat [12]. These defensive techniques may include coping responses that diminish fear, for example, avoiding the message, minimizing the severity of the threat, or denying its relevance [5, 12, 28]. As a consequence, Keller and Block [12] recommended that, interventions that minimize elaboration of message-related problems should enhance the persuasion impact of messages with high-fear appeals.

A different process appears to be effective for the persuasion effects of low-fear appeals. Low fear arousal diminishes persuasion because there is insufficient elaboration of the harmful consequences of engaging in the destructive behavior [12]. In these cases, interventions that increase the level of problem elaboration should provide the motivation necessary for processing of the message-related problems and thus should enhance its impact on persuasion [12].

2.2 Fear Arousal and Self-View Interaction

Social cognition research on the self has developed a variety of theoretical constructs to explain the complex nature of self-related behavior. One important aspect of self conceptualization is related to two aspects of self-view – independent and interdependent selves, which reflect the extent to which individuals view themselves either as an individuated entity or in relation to others [16, 23]. People with independent self-view, tend to focus on the personal self, thinking of themselves in terms of unique personal traits and attributes and de-emphasizing others. In contrast, people with interdependent self-view see themselves as part of a group and perceive themselves as being interconnected with and interrelated to others in their social context. The two selves (independent and interdependent) may coexist within every individual and in any culture [9] [17] but individuals may differ in the relative strength of these two selves on a chronic basis (due to social or cultural surroundings), or on a temporarily accessible basis (due to primed or contextually activated self) [9] [17]. That is to say, while specific social or cultural surroundings may encourage the chronic activation of one self, priming can make the other, latent self temporarily accessible. In this study, we focus on differences in self-view due to the primed activated self (i.e., latent self perceptions).

Latent self-view is an important factor in the formation of security related attitudes as demonstrated in [1] and [2]. The decision to practice secure computing behavior has ramifications not only for an end user but also for all the others who access, use, administer, and maintain information resources within the organization. As such, in the present study, we use the self-view manipulations that involve priming an individual to either think of herself as distinct and separate from others (independent self), or to think of herself as part of a larger group (interdependent self).

Prior studies suggest that self-view is a viable means of varying problem elaboration [12]. Information about self includes a vast array of knowledge (e.g., past experiences, values, attitudinal likes and dislikes, and relationships toward others), that "renders the self a source of one of the richest and most elaborate networks in memory" [12]. Because people have more knowledge about themselves than they have about others, message-related problems encoded with respect to the self can be made more elaborate than with problems encoded with respect to a collective [3, 7, 12].

Based on earlier discussion about the relationship between elaboration and fear appeals, we argue that self-view and fear appeals are likely to influence the persuasiveness of security communication in a collective manner. For a high-fear appeal, interventions that reduce elaboration on the message-related problems will increase persuasion. Moreover, we expect less elaboration when the problem is directly related to a collective rather than the self. Thus, the high-fear appeal should be more persuasive than the low-fear appeal when end users are primed with an interdependent self-view. By contrast, interventions that increase elaboration on the message-related problems will increase persuasion for a low-fear appeal. As we expect greater elaboration when the problem is directly related to the self rather than a collective, we predict that the low-fear appeal should be more persuasive than the high-fear appeal when end users are primed with an independent self-view. Therefore, we hypothesize that the fear appeal and self-view manipulations will interact to influence the persuasiveness of security communication:

Hypothesis 1: The high-fear appeal should be more persuasive than the low-fear appeal when subjects are primed with an interdependent self-view.

Hypothesis 2: The low-fear appeal should be more persuasive than the high-fear appeal when end users are primed with an independent self-view.

3. METHOD

3.1 Experiment Design and Subjects

To test the research hypotheses, an experiment will be adopted as the methodology to study the influence of fear appeal and self-view on the compliance intentions of end users with recommendations to enact specific personal computer security actions toward the amelioration of threats. A specific type of threat – spyware — will be introduced in the experiment and end users' compliance intentions of using anti-spyware will be examined as an outcome in the study. Spyware is illicit code that has been surreptitiously placed on a host computer by a foreign agent [22]. Spyware is an increasingly notorious and noxious form of malware found in nearly all computing settings because of its potential to monitor and capture sensitive information from an unprotected computer system by sending that information over the Internet without the knowledge of the host [22].

The experimental treatments will be administered in a 2 (low fear/high fear) × 2 (independent self/interdependent self) between subject design. Faculty, staff and students from a large eastern university will be invited for participation through the Information Technology Services (ITS) in the university. Although we would not argue that the university sample is highly generalizable to the overall population, we believe that this is an appropriate group for the objective of this study and it could be generalized to university settings and to professional and administrative knowledge workers in industry and not-profits.

3.2 Manipulation

In accordance with the design of fear appeal most commonly used in previous research [4, 5], two major elements will be considered: threats (e.g., spyware attack) and recommendations to address threats (e.g., anti-spyware). High-fear appeal and low-fear appeal manipulations will be reflected by two versions of a message that communicate different levels of severity and probability of spyware threats. With regard to the manipulation of self-view, the messages will be worded in such a way to focus either on the individual (e.g., yourself, your data, your personal productivity, etc.) or on the individual as part of a group (e.g., all users of the university, the community, etc.). The content of the anti-spyware messages will be developed based on the examples of spyware awareness programs across non-profit Web sites such as the Department of Homeland Security, National Cyber Security Alliance (NCSA) and EDUCASE.

3.3 Measures

Subjects will be run in large groups with all four conditions randomized within each group. A questionnaire will be administered after subjects read the security messages. Subjects will indicate the level of message persuasion on the basis of their agreement with the message's solution. Three seven-point semantic differential attitudinal scales will be used to measure subjects' estimates of whether they are likely to follow the recommendations to use anti-spyware, how interested they would be in learning more about the anti-spyware, and whether they want to receive an additional information on the anti-spyware.

Several additional measures will be included as possible covariates: gender, propensity to fear, frequency of being attacked by spyware, familiarity with anti-spyware software, whether anyone the subject knew had suffered from spyware attack, whether the subject had tried/adopted the anti-spyware software before.

To assess the adequacy of the fear arousal manipulation, subjects will indicate the degree to which the message made them feel very unafraid/very afraid, relaxed/tense, calm/agitated, and restful/excited on a seven-point semantic differential scale. As the manipulation check for self-view, subjects will be asked if they notice that the messages refer to an individual and his/her actions versus groups of people and their collective actions.

4. FUTURE WORK AND CONCLUSION

In future work, we expect to complete the experiment design, run a pilot test, and execute the experiment. Upon collecting the data, we will analyze them using ANOVA to test the research hypotheses. The overall goal of this study is to better understand how end users can be motivated to practice secure computing. The potential impacts of an end user's security compliance behavior are not isolated to that end user. All the others who access, use, administer, and maintain information resources within an organization and the whole organization stand to suffer if the business productivity will be affected due to security breaches leading to a loss of sensitive data, customer confidence and financial losses. To the extent end users can be reached and their security behaviors improved, the whole organization stands to benefit. Drawing upon research from marketing, information systems and social psychology, we argue that it is possible to influence security behavioral intentions of end users with fear appeal and self view manipulations made salient to end users. This study will represent a logical next step which takes the understanding of what motivates a user to behave in a secure fashion and uses it to frame a message aimed at amplifying the incidence of the desired behavior. In conclusion, the present work together with completed results will give security management a set of practical courses of actions and suggest ways that HCI practitioners and researchers can explore the domain of security communications. Using the groundwork laid down in this study, future data collection and analysis could contribute to extending our theoretical understanding and practical ability to increase persuasiveness of IT security communication.

5. REFERENCES

[1]. Anderson, C.L., *Creating the conscientious cybercitizen: An examination of home computer users' attitudes and intentions*

towards security, in *Conference on Information Systems & Technology (CIST)*. 2005: San Francisco, CA.

[2]. Anderson, C.L. and Agarwal, R. *Practicing Safe Computing: Message Framing, Self-View, and Home Computer User Security Behavior Intentions*. in *International Conference on Information Systems* 2006. Milwaukee, WI.

[3]. Burnkrant, R.E. and Unnava, H.R., *Effects of self-referencing on persuasion.* Journal of Consumer Research, 1995. 22: p. 17-26.

[4]. Eagly, A.H. and Chaiken, S., *The Psychology of Attitudes*. 1993, Fort Worth, TX: Harcourt Brace Jovanovich.

[5]. Eagly, H.A. and Chaiken, S., *Attitude structure and function*, in *The Handbook of Social Psychology* D.T. Gilbert, S.T. Fiske, and G. Lindzey, Editors. 1998, McGraw-Hill: New York. p. 269-322.

[6]. Gordon, L.A., et al., *2006 CSI/FBI computer crime and security survey*, in *Computer Security Institute* 2006. p. 1-26.

[7]. Greenwald, A.G. and Pratkanis, A.R., *The self*, in *Handbook of social cognition*, J. R.S. Wyer, & T.K. Srull, Editor. 1984, Erlbaum.: Hillsdale, NJ. p. 129-178.

[8]. Haefner, D., *Some Effects of Guilt-arousing and Fear-arousing Persuasive Communications on Opinion Change.* American Psychologist, 1956(August): p. 356.

[9]. Hong, Y.-Y., et al., *MulticulturalMinds: A Dynamic Constructivist Approach to Culture and Cognition.* American Psychologist, 2000. 55(July): p. 709–720.

[10]. Janis, I.L. and Feshbach, S., *Effects of fear-arousing communications.* The Journal of Abnormal and Social Psychology, 1953. 48: p. 78-92.

[11]. Janis, I.L. and Terwilliger, R.F., *An experimental study of psychological resistances to fear-arousing communications.* Journal of Abnormal and Social Psychology 1962. 65: p. 403-410.

[12]. Keller, A.P. and Block, G.L., *Increasing the Persuasiveness of Fear Appeals: The Effect of Arousal and Elaboration.* Journal of Consumer Research, 1996. 22(March): p. 448-459.

[13]. Leventhal, H., *Findings and theory in the study of fear communications*, in *Advances in Experimental Social Psychology*, L. Berkowitz, Editor. 1970, Academic Press: New York, NY.

[14]. Leventhal, H. and Niles, P., *A field experient on fear arousal with data on the validity of questionnaire measures.* Journal of Personality, 1964. 32(September): p. 459-479.

[15]. Leventhal, H. and Singer, R.P., *Affect arousal and positioning of recommendations.* Journal of Personality and Social Psychology, 1966. 4: p. 137-146.

[16]. Markus, H., *Self-schemata and processing information about the self.* Journal of Personality and Social Psychology, 1977. 35(August): p. 63-78.

[17]. Markus, H.R. and Kitayama, S., *Culture and the Self: Implications for Cognition, Emotion, and Motivation.* Psychological Review, 1991. 98(April): p. 224–253.

[18]. Ortony, A. and Turner, T.J., *What's basic about basic emotions?* . Psychological Review, 1990. 97: p. 315-331.

[19]. Pahnila, S., Siponen, M., and Mahmood, A., *Employees' Behavior towards IS Security Policy Compliance*, in *Proceedings of the 40th Hawaii International Conference on System Sciences*. 2007, IEEE Computer Society: Big Island, HI, United States.

[20]. PrivacyRights. *A Chronology of Data Breaches, Privacy Rights Clearinghouse*. 2007 [cited; Available from: http://www.privacyrights.org/ar/ChronDataBreaches.htm.

[21]. Rhee, H.-S., Ryu, Y.U., and Kim, C.-T. *I am fine but you are not: Optimistic bias and illusion of control on information security*. in *International Conference on Information Systems*. 2005. Las Vegas, NV.

[22]. Schmidt, M.B. and Arnett, K.P., *Spyware: A little knowledge is a wonderful thing.* Communications of the ACM, 2005. 48(8): p. 67-70.

[23]. Singelis, T.M., *The Measurement of Independent and Interdependent Self-Construals.* Personality and Social Psychology Bulletin, 1994. 20(October): p. 580-591.

[24]. Singer, E., *Key Concepts in Psychotherapy*. 1965, New York: Basic Books.

[25]. Siponen, M., *A Conceptual Foundation for Organizat ional Information Security Awareness.* Information Management & Computer Security,, 2000. 8(1): p. 31-41.

[26]. Sternthal, B. and Craig, C.S., *Fear Appeals: Revised and Revisited.* Journal of Consumer Research, 1974. 1(3): p. 22-34.

[27]. von Solms, R. and von Solms, B., *From policies to culture.* Computers and Security, 2004. 23(4): p. 275-279.

[28]. Witte, K., *Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeal successes and failures*, in *Handbook of Communication and Emotion: Research, Theory, Applications, and Contexts*, P.A. Andersen and L.K. Guerrero, Editors. 1998, Academic Press: San Diego, CA.

[29]. Woon, I.M.Y., Tan, G.W., and Low, R.T. *A Protection Motivation Theory Approach to Home Wireless Security*. in *International Conference on Information Systems*. 2005. Las Vegas, NV.