FACTORS INFLUENCING AWARENESS OF COMPUTER USAGE POLICIES

C. Bryan Foltz
Department of Computer Science and Information Systems, College of Business and Public Affairs, University of Tennessee at Martin, 8 Business Building, Martin, TN 38238, foltz@utm.edu, (731) 881-7481

John E. Anderson
Department of Management Information Systems, College of Business, East Carolina University, 3410 Bate Building, Greenville, NC 27858, andersonj@ecu.edu, (252) 328-5351

Paul H. Schwager
Department of Management Information Systems, College of Business, East Carolina University, 3410 Bate Building, Greenville, NC 27858, schwagerp@ecu.edu, (252) 737-1050

ABSTRACT

Organizations depend on computer usage policies to protect their information assets, limit liability, and protect employees. However, anecdotal evidence suggests that many individuals are not aware of these policies and what they contain. This pilot study is an initial step in a study designed to improve our understanding of individuals' awareness and perceptions of these policies and why many individuals elect not to read computer usage policies.

INTRODUCTION

Information systems misuse and computer crime is a serious and ongoing problem in the modern computing environment. Although the 2004 CSI/FBI Computer Crime and Security Survey (Gordon, Loeb, Lucyshyn, and Richardson, 2004) suggests that the cost and frequency of misuse and computer crime is declining, the problem still remains significant. One approach to computer security focuses upon the use of computer usage policies, which are viewed as the cornerstone of computer security (Backhouse and Dhillon, 1995). However, existing research suggests that many users simply don't read these policies (Foltz, Cronan, and Jones, 2004).

Computer Use Policies

A Computer Use Policy (CUP) defines who is allowed to use computer facilities and how those facilities may be used in an organization. It is the organization's official position on computer use. It can be a platform to develop a group ethic for computer users (Scott and Voss 1994).

CUPs were developed in response to legal and security issues, employee and employer rights, and fairness. A CUP commonly contains seven elements: 1) monitoring use of proprietary assets, 2) establishing no expectation of privacy, 3) improper employee use, 4) allowable employee uses, 5) protecting sensitive company information, 6) disciplinary action, and 7) employee acknowledgement of policy (Holmes 2003). By giving legal notice, instructing in expected use and disciplinary actions, and requiring acknowledgement, CUPs should deter misuse. However, CUPs are only effective if they are read, understood, and obeyed.

Purpose

Given the importance of computer usage policies, the tendency of individuals to not read such policies is concerning. The purpose of this research is to investigate why individuals elect not to read such policies. An understanding of why people fail to read such policies is a first step in increasing the effectiveness of these policies.

LITERATURE REVIEW

A significant amount of research regarding information systems security has accumulated over the years. For example, numerous authors have examined the frequency and cost of IS misuse and computer crime. Also, a number of approaches to preventing misuse have been considered. Unfortunately, no research exploring why individuals elect not to read usage policies was found. However, research explaining human behavior does exist.

Frequency and Cost of IS Misuse and Computer Crime

Both the frequency and the cost of IS misuse and computer crime have frequently been evaluated. The National Center for Computer Crime Data estimated the yearly cost at $555 million (Romney, 1995). Other authors have resisted the temptation to place dollar estimates on the cost of misuse, instead suggesting that the cost of misuse is in the millions or billions of dollars annually (Straub and Nance, 1990). Other studies have evaluated the frequency of misuse. For example, the American Society for Industrial Security found that the frequency of loss caused by IS misuse and computer crime jumped 323 percent from 1992 to 1996 (Anthes, 1996).

However, recent CSI/FBI surveys suggest a change in this trend. The 2004 CSI/FBI Computer Crime and Security survey suggests that the frequency of successful attacks on systems has been declining since 2001, noting that only 53% of respondents reported unauthorized system use. Further, the 2004 CSI/FBI survey also suggests that total losses from IS misuse and computer crime are falling (the 2003 survey reported total costs of $201,797,340, while the 2004 survey reported total costs of $141, 495,560). Although this would seem to be good news, the frequently-cited CSI/FBI surveys are also subject to criticism from a number of sources. For example, Flickes (2004) notes that the CSI/FBI survey does not track respondents from year to year and thus the trends reported by the survey may be inaccurate. Flickes also notes that the financial losses reported in the CSI/FBI survey are inconsistent with a U.S. Secret Service survey, which estimated losses of $666 million. Other authors express concern over the CSI/FBI sample (Heiser, 2002). Despite these concerns with specific survey instruments, IS misuse and computer crime is clearly an ongoing problem that must be addressed by organizations.

Approaches to Preventing Information Systems Misuse and Computer Crime

The ongoing concern with IS misuse and computer crime has resulted in the development of several computer security models. Krause and Tipton (1998) point out that some of these models, such as the Bell-LaPuda model, the Biba integrity model, the Clark-Wilson model, the Goguen-Mesequer model, the Southerland model, and the Brewer-Nash model, focus on the traditional CIA (confidentiality, integrity, availability) framework; while others utilize behavioral or criminological theory. While the CIA models are interesting, the behavioral and criminological theory models are of particular interest to this study since these models assume user familiarity with computer usage policies.

Straub's Computer Security Model

Straub's Computer Security Model (Straub, 1986) is especially relevant to the current research since it assumes that users are familiar with organizational computer usage polices. The Computer Security Model (CSM) also suggests that organizations need multiple layers of protection against misuse. These layers include deterrents, preventives, and detectives (Straub, 1986). Deterrents are based on the Theory of General Deterrence (TGD) and are essentially policies explaining acceptable and unacceptable uses of organizational information systems (Straub, 1986). Past research suggests that deterrents do help reduce misuse in organizations (Klette, 1975; Straub, 1987). Deterrents are primarily effective in blocking misuse perpetrated by insiders. The second layer of the CSM, preventives, consists of active measures such as passwords and encryption. Since these methods actively limit access to the system and to data (Straub, 1986), they are effective at preventing misuse conducted by insiders and outsiders alike. The final layer of the CSM, detectives, is designed to detect misuses after they occur so that recovery can begin (Straub, 1986).

Theory of General Deterrence

The deterrent portion of the CSM is based upon the Theory of General Deterrence (TGD). The idea of using the threat of punishment to prevent unacceptable behavior such as crime can be traced to Bentham in the 18th century (Nagin, 1978). Deterrence is "the preventive effect which actual or threatened punishment of offenders has upon potential offenders" (Buikhuisen, 1974, p285). Nagin (1978, p. 96) further defines general deterrence to mean that "the imposition of sanctions on one person may demonstrate to the rest of the public the expected costs of a criminal act, and thereby discourage criminal behavior in the general population." The sanctions mentioned above are typically measured by examining two constructs: the certainty and severity of sanction.

Although the TGD represents one approach to preventing specific behavior, the theory assumes that individuals are fully aware of sanctions (Blumstein, Cohen, and Nagin, 1978). Existing research suggests that this is not true (Foltz, Cronan, and Jones, 2004; Assembly Committee on Criminal Procedure (State of California), 1975.) To understand human behavior toward an action, such as reading or not reading CUPs, we may consider more fundamental behavior models, specifically the Theory of Planned Behavior (Ajzen, 1991), Social Trust, and Apathy.

APPROACHES TO UNDERSTANDING AND PREDICTING HUMAN BEHAVIOR

Theory of Planned Behavior

The TPB suggests that behavior can be predicted by examining individual intention to commit that behavior and individual perceptions regarding control of that behavior (Ajzen, 1988; 1991; Doll and Ajzen, 1992). Intentions "are assumed to capture the motivational factors that influence a behavior" (Beck and Ajzen, 1991, p. 286) and indicate the degree of effort individuals are willing to exert to perform the behavior. In the TPB, three variables are theorized to be determinants of intention and behavior: 1) Attitude Toward Behavior (individual's positive or negative feelings about performing the target behavior), 2) Subjective Norm (individuals' perception that most people important to him think he should or should not perform the behavior), 3) Perceived Behavioral Control (perceived ease or difficulty of performing the behavior) (Ajzen, 1991). Perceived behavioral control incorporates individual perception of information, skills, abilities, emotions, compulsions, opportunity, and dependence upon others (Ajzen, 1988).

The TPB variables may influence an individual's decision to read a computer usage policy. An individual may have negative attitudes toward such policies, may perceive that others think he should read them, and/or may perceive the reading of such policies as difficult. TPB has been applied to individual acceptance and usage in many technology contexts (Harrison et al 1997; Mathieson 1991; Taylor and Todd 1995).

Social Trust

The Theory of Planned Behavior does not specifically deal with individual expertise in technical areas, although the perceived behavioral control factor does incorporate an idea of ability to perform the behavior. However, many individuals substitute social trust for knowledge of risks associated with technology (Earle and Cvetkovich, 1995). Social trust is the willingness to rely on those who have the responsibility of making important decisions related to the management of technology, the environment, medicine, etc., especially where an individual lacks the interest, time, abilities, knowledge, or other resources to personally make decisions (Siegrist, Cvetkovich, and Roth 2000).

Social trust may influence an individual's decision to read computer usage policies. If an organization provides well-trained individuals to cope with IS security threats, users may simply feel there is no need for them to invest time reading the policies, since specific individuals with (we assume) greater knowledge and training are already responsible for protecting the systems. Thus, some individuals may decide not to read the policies.

Apathy

In addition to the variables of TPB and Social Trust, apathy is another possible determinant of intention and behavior of reading usage policies. Apathy is often defined as lack of motivation, interest, and emotion (Robert et al 2002). An individual may have read policies at an earlier time but currently no longer reads them, may have no interest in reading them, and may feel they have nothing really to do with him.

RESEARCH QUESTIONS AND CONCEPTUAL MODEL

The primary research questions of this study are: 1) do users elect not to read computer use policies as anecdotal evidence suggests, and 2) what are the determinants of a user reading or not reading such policies. To help answer these research questions, a conceptual model combining the TPB, social trust, and apathy was created. This model appears in Figure 1.

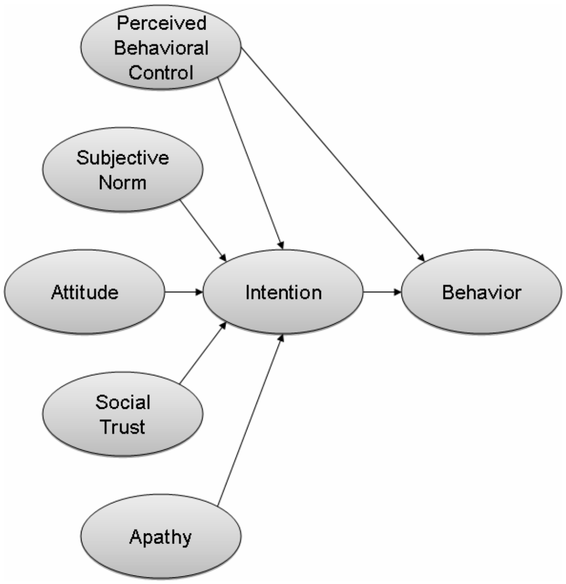

Figure 1

METHODOLOGY

Constructs and Measurement

This study examines relationships among five possible determinants of intention to read computer use policies with intention and use behavior. The TPB constructs of Attitude, Subjective Norm, and Perceived Behavioral Control were measured with Taylor and Todd's (1995) original items and five-point scale adapted to reading computer usage policies. The variable Usage Intention was measured with Madden, Ellen, and Ajzen's (1992) and Beck and Ajzen's (1991) items. The variable Use Behavior was measured using a 10-point Likert scale. Two items were used: one evaluates the percentage of time respondents read computer use policies completely, while the second evaluates the percentage of time respondents simply skimmed computer use policies. Social Trust was measured using the items from Siegrist (2000), Siegrist, Cvetkovich and Roth (2000); and Siegrist and Cvetkovich (2000). Apathy was operationalized by five questions measuring interest, emotions, and motivation on a 5-point scale.

Data Collection

Data for this study is being collected utilizing a web-based survey administered to students in MBA classes and in introductory information systems classes. Students in the introductory classes are from a variety of majors and represent many different life experiences. For the purposes of this pilot research, students represent an appropriate sample.

At the start of the survey students are greeted by a short letter informing them that participation is voluntary and anonymous. At the end of the letter is a text box for an access code. Students will enter a set code to access the survey. Use of this code will help insure that only those asked to participate actually participate. This will also be useful in helping calculate the response rate.

Hypotheses

To answer the research questions posed earlier, a variety of hypothesis will be tested.

H1. Perceived control will positively affect behavior.

H2. Subjective norm will positively affect behavior.

H3. Attitude will positively affect behavior.

H4. Social Trust will positively affect behavior.

H5. Apathy will negatively affect behavior.

RESULTS

Initial results from this exploratory study are promising indeed. An examination of the structural model using Smart PLS indicates that the model explains approximately 50% of the variability in behavior (R^2 = .498). These results are based upon 46 responses from students enrolled in an MBA-level information systems class (46 of 83 students responded to the survey, for a 55% response rate). Further, a measurement model of the five main constructs was estimated using reflective indicators. Construct reliability was assessed using composite reliability. All but two of the construct reliabilities exceeded Nunnally's (1978) suggested .7 benchmark (Attitude = .67 and Social Trust =.59). Convergent validity was examined using the average variance extracted measure. Unfortunately, most constructs fell short of Fornell and Larcker's (1981) suggested .5 benchmark. For example, Perceived Behavioral Control generated an AVE score of .49, while the scores for Apathy, Social Trust, and Attitude were .46, .31, and .24, respectively.

In addition, each of the five hypotheses was examined using t-tests (40 degrees of freedom). Three of the hypotheses were supported, while two were not. H1 is supported at the .1 level (t-value = 1.54, β = 0.114). Perceived Behavioral Control does affect behavior. H3 is also supported at the .05 level (t-value of 2.248, β =0 .307), suggesting that attitude does influence behavior. Also, H5 is supported at the .1 level (t-value of 2.04, β = -0.25), suggesting that apathy does negatively affect behavior. H2 and H4 were not supported, suggesting that Subjective Norm and Social Trust do not influence behavior (H2 t-value of 0.874, β = 0.079, H4 t-value of 1.267, β = 0.115). The results are shown in Figure 2.

The purpose of this research is to investigate why individuals elect not to read such policies. The results of this exploratory study suggest that respondents are unconcerned with the opinions of others (Subjective Norm) and are not simply trusting others to make decisions for them (Social Trust). However, respondents are comfortable with their ability to read and understand computer use policies (Perceived Behavioral Control), but do not feel inclined to read the policies (Attitude and Apathy).

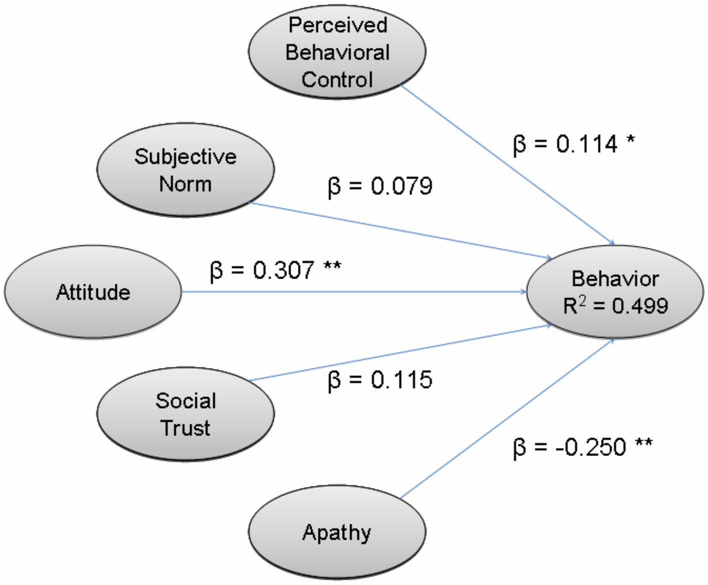

Figure 2

CONCLUSIONS AND DIRECTIONS FOR FUTURE RESEARCH

This exploratory research examines a model intended to explain why individuals elect not to read computer usage policies. The model, while imperfect, explains almost 50% of the variance in the dependent variable. This is a solid result for an exploratory study; however, a number of issues remain to be examined. For example, the sample consisted only of MBA students at one university. The scope of the sample must be enlarged to include a more representative cross section of individuals. However, the most interesting result of this research is the impact of apathy and attitude upon the decision to read computer usage policies. Since computer usage policies are considered the cornerstone of computer security (Backhouse and Dhillon, 1995), future research must further examine the impact of apathy and attitude upon this decision. Finally, a method for overcoming this apathy must be found.

REFERENCES

Ajzen, Icek. (1988). Attitudes, Personality, and Behavior. The Dorsey Press, Chicago, IL.

Ajzen, Icek. (1991). "The Theory of Planned Behavior." *Organizational Behavior and Human Decision Processes*, 50(2), pp. 179-211.

American Bar Association. (1984). "Report on Computer Crime", pamphlet prepared by the Task Force on Computer Crime, American Bar Association, Section on Criminal Justice, 1800 M Street, Washington, D.C., 20036.

Anthes, Gary H. (1996). "Hack Attack: Cyberthieves Siphon Millions from U.S. Firms." *Computerworld*, 30(16), p. 81.

Backhouse, James and Gurpreet Dhillon (1995). "Managing Computer Crime: A Research Outlook." *Computers and Security*, 14(7), 645-651.

Beck, Lisa and Icek Ajzen. (1991). "Predicting Dishonest Actions Using the Theory of Planned Behavior." *Journal of Research in Personality*, 25(3), pp. 285-301.

Blumstein, Alfred, Jacqueline Cohen, and Daniel Nagin, Eds. Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates. National Academy of Sciences, Washington, D.C., 1978.

Bort, Julie (2002). "Time for a New Security Model." *Network World*, 19(30), pp. s6-8.

Buikhuisen, W. (1974). "General Deterrence: Research and Theory." *Abstracts on Criminology and Penology*, 14(3), pp. 285-288.

Doll, Jork and Icek Ajzen. (1992). "Accessibility and Stability of Predictors in the Theory of Planned Behavior." *Journal of Personality and Social Psychology,* 63(5), pp. 754-764.

Dutta, Amitava and Kevin McCrohan. (2002). "Management's Role in Information Security in a Cyber Economy." *California Management Review*, 45(1), Fall, pp. 67-87.

Earle, T. and Cvetkovich G. (1995). Social trust: Toward a cosmopolitan society. Westport, CT: Praeger.

Flickes, Michael. (2004). "Behind the Numbers: The FBI Cyber-Crime Survey Results." Government Security web site, http://govtsecurity.com/mag/behind_numbers_fbi/. August 1, 2004.

Foltz, Charles, Timothy. Paul Cronan, and Thomas Jones (2002). "Human Behavior as a Factor in the Control of Information Systems Misuse and Computer Crime." Proceedings of the Decision Sciences Institute, pp. 1246-1251.

Foltz, Charles B., Timothy Paul Cronan, and Thomas W. Jones (2004). "Student Awareness of University Computer Usage Policies: Is a Single Exposure Enough?" Proceedings of the Southwest Decision Sciences Institute, Orlando, FL, pp. 293-299.

Fornell, C. and Larcker, D. (1981). "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error." *Journal of Marketing Research*, 18, pp. 89-98.

Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Robert Richardson. (2004). 2004 CSI/FBI Computer Crime and Security Survey. Computer Security Institute.

Heiser, Jay. (2002). "Can You Trust Infosecurity Surveys?" Curmudgeon's Corner Column, Information Security, http://infosecuritymag.techtarget.com/2002/apr/curmudgeon.shtml.

Holmes, J. (2003). "Formulating an effective computer use policy." *Information Strategy: The Executive's Journal*, 20(1), 26-33.

Klette, H. (1975) "Some Minimum Requirements for Legal Sanctioning Systems with Special Emphasis on Detection." General Deterrence: A Conference on Current Research and Standpoints. National Swedish Council for Crime Prevention, Stockholm, pp. 12-59.

Krause, Micki, and Harold F. Tipton, editors. (1998). Handbook of Information Security Management, Auerbach,

LaPadula, Leonard J. (1996) "Forward." *Journal of Computer Security*, 4, pp. 233-238.

Lee, J. and Lee, Y. (2002) "A Holistic Model of Computer Abuse within Organizations." *Information Management and Computer Security*, 10(2), pp. 57-63.

Madden, Thomas J., Pamela Scholder Ellen, and Icek Ajzen. (1992). "A Comparison of the Theory of Planned Behavior and the Theory of Reasoned Action." *Personality and Social Psychology Bulletin*, 18(1), pp. 3-9.

Manski, Charles F. (1978). "Prospects for Inference on Deterrence through Empirical Analysis of Individual Criminal Behavior." Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates. Ed. Afred Blumstein, Jacqueline Cohen, and Daniel Nagin. National Academy of Sciences, Washington, D.C., pp. 400-424.

Nagin, Daniel. (1978). "General Deterrence: A Review of the Empirical Evidence." Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates. National Academy of Sciences, Washington, D.C., pp. 93-139.

Nunnally, J. (1978). Psychometric Theory (2nd ed.) New York, NY: McGraw-Hill.

Peace, A.G., D. F. Galletta, and J. Y.L. Thong. (2003). "Software Piracy in the Workplace: A Model and Empirical Test." *Journal of Management Information Systems*, 20(1), pp. 153-177.

Romney, Marshall. (1995). “Computer Fraud--What Can Be Done About It?” *The CPA Journal*, 65(5), pp. 30-33.

Scott, T., and Voss, R. (1994). Ethics and the 7 “P’s” of computer use policies. Proceedings of the conference on Ethics in the computer age, Gatlinburg, TN, ACM 61-67

Siegrist, M. (2000). “The Influence of Trust and Perceptions of Risks and Benefits on the Acceptance of Gene Technology.” *Risk Analysis*, 20(2), 195-203.

Siegrist, M., Cvetkovich, G., and Roth, C. (2000). “Salient value similarity, social trust, and risk/benefit perception.” *Risk Analysis*, 20(3), 353-362.

Siegrist, M., and Cvetkovich, G. (2000). “Perception of hazards: the role of social trust and knowledge.” *Risk Analysis*, 20(5), 713-719.

Straub, D. W. (1986). Deterring Computer Abuse: The Effectiveness of Deterrent Countermeasures in the Computer Security Environment. Indiana University Graduate School of Business, Dissertation.

Straub, D. W. (1987) “Controlling Computer Abuse: An Empirical Study of Effective Security Countermeasures.” Proceedings of the International Conference on Information Systems, pp. 277-289.

Straub, Detmar W. and William D. Nance. (1990). “Discovering and Disciplining Computer Abuse in Organizations: A Field Study.” *MIS Quarterly*, 14(1), pp. 45-60.

Taylor, S., and Todd, P.A. (1995). “Understanding Information Technology Usage: A Test of Competing Models.” *Information Systems Research*, 6(2), 144-176

Vankatesh, V., Morris, M., Davis, G., and Davis, F. (2003). “User Acceptance of Information Technology: Toward a Unified View.” *MIS Quarterly*, 27(3), p. 425-478.