SAIS 2005 Proceedings

Southern (SAIS)

3-1-2005

Faculty Awareness of University Computer Usage Regulations

Bryan Foltz
foltzc@mail.ecu.ecu

Richard Hauser

Recommended Citation

Foltz, Bryan and Hauser, Richard, "Faculty Awareness of University Computer Usage Regulations " (2005). *SAIS 2005 Proceedings*. 9.
http://aisel.aisnet.org/sais2005/9

FACULTY AWARENESS OF UNIVERSITY COMPUTER USAGE REGULATIONS

Bryan Foltz
East Carolina University
foltzc@mail.ecu.ecu

Richard Hauser
East Carolina University
hauserr@mail.ecu.edu

Abstract

This study examined faculty awareness of computer usage regulations in the following areas: awareness, diffusion, effectiveness, and perception of the security environment. In addition, the concept of social trust as it relates to computer security was explored. In general, the survey found respondents to be rather neutral in regards to their knowledge of computer security regulations. They also tended to have less confidence in their peers' or students' knowledge of these regulations. Not surprisingly, those who perceived the risk of computer misuse to be high were more likely to discuss it with their students. The most interesting part of this study lies in the concept of social trust as it relates to computer security. Our results provide some support for the notion that many faculty members may simply fail to read the policies since other, potentially more knowledgeable, individuals are in charge of preventing computer misuse

Keywords: Security, computer usage policy, computer misuse, social trust

Introduction

While computers have increasingly become indispensable in both business and education, incidences of both computer security violations and misuse are occurring at an alarming rate. Security violations run the gamut from denial of service and viral attacks to information theft. In fact, the security incident rate now doubles every year (Piscitello and Kent, 2003). The 2002 CSI/FBI Computer Crime and Security Survey recently found that over 90% of respondents had detected security breaches, up from 85% the prior year (Power, 2002). Power (2002) also notes that the cost of these incidents has increased dramatically. Although only 44% of respondents quantified financial losses due to these incidents, the total losses reported totaled $455.8 million, up from $377.8 million in the 2001 survey.

Universities may be even more susceptible to security violations. The unique nature of the teaching/learning/research environment requires a large number and variety of computing platforms, networks, and software packages. Many times, faculty, staff, or students may not be aware of the nature of the networks on which they install software. This can lead to inadequate security procedures that can leave the system open to security breaches (Rezmierski et al., 2002).

In addition, universities are also besieged by incidents of misuse including peer to peer file sharing, accessing inappropriate websites, and copyright infringement.. At the University of Florida, for example, 3,500 simultaneous connections to Kazaa were recorded last year (King, 2003). Obviously this is both a legal and bandwidth problem.

In an attempt to limit these problems, many universities have instituted written computer usage policies for faculty, staff, and students. Gaining awareness of these policies has sometimes proved difficult. Students, in particular, often obtain information about computer security regulations from student handbooks, campus newspaper articles, and word of mouth. More importantly, students often look to faculty for information regarding proper computer use. It is important, therefore, that faculty be aware of and understand computer usage policies. For that reason, this research investigates faculty awareness of those policies.

Computer Usage Policies

Computer usage policies are considered the cornerstone of computer security (Backhouse and Dhillon, 1995). These written policy statements detail acceptable and unacceptable uses of an organizational information system, and often contain information regarding sanctions for unacceptable use as well. Such statements are thought to reduce the performance of misuse within organizations (Straub, 1987).

Computer usage policies are based on the Theory of General Deterrence (Harrington, 1996). The Theory of General Deterrence (TGD) suggests that punishing an offender will prevent others from committing the same action. In short, "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" (Nagin, 1978, p. 96).

However, most computer usage policies share one critical assumption with the TGD. These policies, like the TGD, assume that individuals are familiar with the policies and sanctions in question. Unfortunately, existing research suggests that most individuals are not aware of actual sanctions (Assembly Committee on Criminal Procedure (State of California), 1975). As a result, many TGD researchers have recommended focusing on perceived rather than actual sanctions (Andenaes, 1975; Anderson, 1979; Chiricos and Waldo, 1970; Gibbs, 1975; Henshel and Carey, 1975; Williams and Hawkins, 1986).

In short, the existence of computer usage policies within an organization or university may have little effect on the performance of computer misuse if the users are unfamiliar with such policies. Rather, research examining computer misuse should focus on user perceptions of policies, rather than upon the actual policies themselves.

Student Awareness of University Computer Usage Policies

Within the university setting, computer usage policies are used to inform students and employees of acceptable and unacceptable uses (and sanctions) of the academic computing resource. Unfortunately, few universities actually insist that users review the university computer usage policies. Some universities do mention the policies during new student orientation; while others simply insist that all users sign a form agreeing to abide by the policies. Of course, most users sign these forms without actually reading the policies (just as most users install software without actually reading the software license agreement). Thus, many university users are unfamiliar with the university computer usage policies governing their use of the systems.

A recent study evaluated student awareness of university computer usage policies at three midwestern universities (Foltz, Cronan, and Jones, 2004). Less than one fourth of the 416 respondents had read the computer usage policies at their respective universities. In addition, most students were unable to identify methods used by their universities to distribute such policies. Although over half (59%) realized that computer support departments distributed usage policies, only 22% reported classroom distribution of such policies. Further, only 23% reported informal class discussions regarding correct and incorrect usage, while 17% reported informal computer lab discussions about the university computer usage policies. Fewer than 7% reported receiving information about university computer usage policies at organizational (club) meetings. Obviously, most students surveyed were not fully aware of the university computer usage policies.

Prior studies suggest that university students conduct a surprising amount of misuse. For example, Skinner and Fream (1997) found that about half of the respondents to a survey conducted at a southern university acknowledged committing some form of misuse during their lifetimes. In addition, Hollinger (1988) conducted focused interviews with eleven college students, including eight randomly selected from an upper-level computer science course and three known offenders. Of the eight, only four reported "no significant deviant activity" (p. 200) although these four did report occasional trading of stolen (pirated) software. Five of the eight randomly selected students reported many instances of gaining unauthorized access to other student accounts to browse or change data files.

Faculty Awareness of University Computer Usage Policies

While a number of recent studies have focused upon student computer misuse and student awareness of university computer usage policies, no research evaluating faculty awareness of usage policies has been performed. This lack of research is concerning for two reasons. First, faculty members are valid users of university computer systems and thus are also potential misusers. This problem is exaggerated by the greater access often enjoyed by faculty members. For example, faculty members with computers in their offices are able to work without observation at their own convenience - a luxury often denied students working in traditional computer labs. Further, faculty members often have access to sensitive information such as personal records about students and administrative information about other university employees. These factors alone suggest that faculty should be aware of university computer usage policies.

Second, and more importantly, faculty members are both an information source and role model for students. Faculty members often answer student questions regarding university policies. While they are typically not responsible for educating students regarding such policies, an inability to answer such questions may result in improper understanding on the part of students. In addition, faculty should be aware of their leadership role. Their behavior should serve as a guide for students. Thus, faculty members, like all valid users, should be aware of university computer policies.

The importance of faculty members in shaping student behavior is highlighted by the Theory of Planned Behavior (Ajzen, 1988). The Theory of Planned Behavior (TPB) suggests that behavior is best predicted by individual intention to perform that behavior (Ajzen, 1988; 1991; Doll and Ajzen, 1992). Intentions capture motivating factors that influence a behavior (Beck and Ajzen, 1991) and are formed as a result of individual attitudes toward the behavior, subjective norms, and perceived behavioral control (Ajzen, 1988). Attitudes are individual positive or negative evaluations of a behavior (Ajzen, 1988; Doll and Ajzen, 1992), while perceived behavioral control reflects the individuals' perception of their ability to perform the behavior in question (Ajzen, 1988). Subjective norms reflect perceived social pressure to perform or not perform a behavior based on referent others (people important to the individual) (Ajzen, 1988). Thus, the leadership role of faculty members may influence student performance of misuse, assuming that students perceive faculty members as important. Also, the TPB has been tested and supported in the study of misuse (Foltz, Cronan, and Jones, 2002).

Social Trust

One factor that could potentially affect faculty members' awareness of usage policies could be their degree of social trust. Social trust refers to the tendency of laypeople to trust experts to make correct decisions regarding technology. Existing research in the area suggests that experts and laypeople often differ in opinions regarding the benefits and risks of technology hazards, partially because laypeople lack the expertise to correctly understand or evaluate these benefits and risks (Siegrist and Cvetkovich, 2000; Cvetkovich, Siegrist, Murray, and Tragessor, 2002; Siegrist, Cvetkovich, and Roth, 2000). Since most universities provide highly-trained technical support personnel, many faculty members may simply fail to read the policies since other, potentially more knowledgeable, individuals are in charge of preventing computer misuse. Although this seems like a logical decision, the consequences may be a lower level of faculty knowledge regarding university regulations. As mentioned earlier, this could lead to an increased amount of student misuse. For this reason, this study also measures the social trust experienced by faculty members.

Methodology

A questionnaire was developed to investigate the faculty awareness of computer usage policies. The questionnaire includes demographic items, social trust items, and awareness items. The demographics section requests the following information: the Carnegie classification of the university, whether it is public or private, the academic rank of the respondent, the years of academic experience, gender, age, and the total enrollment of the institution. The social trust section utilizes items drawn from existing literature. The awareness portion of the questionnaire uses a survey instrument previously used to examine student awareness of university computer usage policies. It uses a 7 point Likert scale with 1 being strongly agree and 7 being strongly disagree. This instrument was slightly modified to reflect the target population.

The questionnaire was pilot tested using potential members of the target population. After evaluation and modification it was then administered via the internet to randomly chosen faculty members at a large university. In all, 300 faculty members were surveyed and a total of 75 usable responses were received, for a response rate of 25 percent. The results were analyzed using SPSS.

Results

The survey data indicates that the respondents were fairly evenly split among academic departments with a slight majority coming from business or technology. Respondents were also evenly divided by gender, with an average age of 48. The respondents averaged nearly 16 years of academic experience with nearly 11 of that at their current institution. The respondents fell into the following academic categories: assistant professor (37.8%), associate professor (25.7%), full professor (18.9%), and other (16.3%). Most faculty members (71.6%) reported reading the regulations, and with a relatively short average time (8 months) since last reading them.

The results of the perceptual portion of the questionnaire are shown in Table 1. These results are divided into 5 separate areas: Awareness, Diffusion, Effectiveness, Perception of the Security Environment, and Social Trust.

Awareness

In terms of awareness, respondents tended to be neutral on their own awareness of the location of the usage rules. They were, however, less confident that their colleagues knew of the usage rules and even less confident in their students knowledge. Not surprisingly, those who had read the policy were significantly (.006) more aware of its location. Female respondents were significantly (.026) more likely to agree that faculty members were actively made aware of the policies than male.

Diffusion

Respondents were less certain that their colleagues or students had knowledge of the computer usage regulations. Respondents who believed that the threat of misuse was more risky were significantly more likely to discuss the usage policies with their students in both the classroom (.048) and the lab (.003). In addition, those who reported high levels of knowledge about the risk of computer misuse were significantly more likely to discuss the policies in the classroom (.000) or lab (.000).

Effectiveness

Respondents generally agreed with these items, indicating a lack of effectiveness of the usage regulations. Male respondents were more likely to agree that faculty members agreed to the regulations without reading them.

Perception of the Security Environment

Respondents tended to agree with all items in this category. In general, respondents felt that the security philosophy was well meaning, well known, and was formed in a response to known or suspected security incidents.

Table 1. Survey results.

Question (1=strongly agree, 2 = strongly disagree)	**Mean**
Awareness	
I am familiar with the Academic Computer Use Regulations	3.37
I know where the regulations are located.	4.7
Other faculty members know where the regulations are located.	5.0
Students know where the regulations are located.	5.59
Diffusion	
The University insists that faculty members read and reread regulations.	4.65
The University insists that students read and reread regulations	5.10
I discuss regulations with students in the classroom	5.32
I discuss regulations with students in the lab.	5.18
Effectiveness	
Most faculty agree to the regulations without reading them.	2.39
Most students agree to the regulations without reading them.	2.75
Most faculty read the regulations once and then forget about it.	3.23
Perception of the Security Environment	
Security philosophy is to provide tight security without hindering productivity.	3.19

Security efforts are well known.	3.79
Security efforts are in reaction to known or suspected incidents.	3.69
Security efforts convince people not to commit misuse.	3.79

Social Trust

As mentioned earlier, social trust refers to the tendency of laypeople to trust experts to make correct decisions regarding technology. In general, the results support this concept. First, a significant correlation. (000) exists between the level of confidence respondents have in those in charge of computer security and the perceived worth of the policy. Confidence in those in charge of computer security was also positively correlated with confidence in deterrence (.005). Also, respondents with higher levels of confidence in the authorities were significantly (.007) more likely to believe that students agreed to computer policies without reading them. Finally, those with higher degrees of knowledge were significantly (.000) more likely to believe that threats to security were risky.

Conclusion

This study examined faculty awareness of computer usage regulations in the following areas: awareness, diffusion, effectiveness, and perception of the security environment. In addition, the concept of social trust as it relates to computer security was explored.

In general, the survey found respondents to be rather neutral in regards to their knowledge of computer security regulations. They also tended to have less confidence in their peers' or students' knowledge of these regulations. Not surprisingly, those who perceived the risk of computer misuse to be high were more likely to discuss it with their students.

The most interesting part of this study lies in the concept of social trust as it relates to computer security. Our results provide some support for the notion that many faculty members may simply fail to read the policies since other, potentially more knowledgeable, individuals are in charge of preventing computer misuse.

The results of this study should be viewed in light of a number of limitations. First, this was a pilot study using an untested instrument. Second, the sample was obtained from a single university. Finally, the sample could contain some sampling bias since those interested in computer security may have been more likely to reply. More research is needed to further explore this phenomenon. Specifically, the role of social trust in the computer security environment within a university setting needs to be further examined.

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.

Andenaes, Johannes (1975). General Prevention Revisited: Research and Policy Implications. *General Deterrence: A Conference on Current Research and Standpoints*. National Swedish Council for Crime Prevention, Stockholm, 12-59.

Anderson, Linda S. (1979). The Deterrent Effect of Criminal Sanctions: Reviewing the Evidence. *Structure, Law, and Power*. Eds. Paul J. Brentingham and Jack M. Kress. Sage Publications, Beverly Hills, CA.

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

Assembly Committee on Criminal Procedure (State of California) (1975). Public Knowledge of Criminal Penalties. *Perception in Criminology*. Eds. R. L. Henshel and R. A. Silverman. Columbia University Press, New York, NY, 74-90.

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

Baskerville, Richard (1993). Information Systems Security Design Methods: Implications for Information Systems Development. *ACM Computing Surveys*, 25(4), 375-414.

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.

Chiricos, Theodore G. and Gordon P. Waldo (1970). Punishment and Crime: An Examination of Some Empirical Evidence. *Social Problems*, 18(2), 200-217.

Cvetkovich, George, Michael Siegrist, Rachel Murray and Sarah Tragesser (2002). New Information and Social Trust: Asymmetry and Perseverance of Attributions about Hazard Managers. *Risk Analysis*, 22(2), pp. 359-367.

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.

Foltz, Charles B, Timothy Paul Cronan, and Thomas W. Jones (2002). Human Behavior as a Factor in the Control of Information Systems Misuse and Computer Crime. Decision Sciences National Convention, San Diego, CA, 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.

Gibbs, Jack P. (1975). *Crime, Punishment, and Deterrence*. Elsevier Scientific Publishing Co., Inc., The Netherlands.

Harrington, Susan J. (1996). The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. *MIS Quarterly*, 20(3), 257-278.

Henshel, R. L. and S. H. Carey (1975). Deviance, Deterrence, and Knowledge of Sanctions. *Perception in Criminology*. Eds. R. L. Henshel and R. A. Silverman. Columbia University Press, New York, NY, 54-73.

King, Julia. (2003), Preventing P2P Abuse, *Computerworld*, 37(49), 52.

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., 93-139.

Piscitello, David and Stephen Kent (2003). The Sad and Increasingly Deplorable State of Internet Security. *Business Communications Review*, 33(2), 49-53.

Power, Richard (2002). 2002 CSI/FBI Computer Crime and Security Survey. *Computer Security Issues & Trends*, VIII(1), 1-22.

Rezmierski, Virginia, Seese, Marshall, and Nathaniel St. Clair II. (2002) *Computers & Security*, 21(6), 557-564.

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

Schwartz, Karen D. (1997). Hackers Are Ubiquitous, Malicious, and Taken Far Too Lightly, Experts Say. *Government Computer News*, 16(23), 81-82.

Siegrist, Michael and George Cvetkovich. (2000) Perception of Hazards: The Role of Social Trust and Knowledge. Risk Analysis, 20(5), pp. 713-719.

Siegrist, Michael, George Cvetkovich, and Claudia Roth. (2000). Salient Value Similarity, Social Trust, and Risk/Benefit Perception. *Risk Analysis*, 20(3), pp. 353-362.

Williams, Kirk R. and Richard Hawkins (1986). Perceptual Research on General Deterrence: A Critical Review. *Law and Society Review*, 20(4), 545-572.