Why users (fail to) read computer usage policies

C. Bryan Foltz
Department of Computer Science and Information Systems, University of Tennessee at Martin, Martin, Tennessee, USA

Paul H. Schwager
Department of Management Information Systems, East Carolina University, Greenville, North Carolina, USA, and

John E. Anderson
Department of Information Systems and Technology, Utah Valley University, Orem, Utah, USA

Received 22 January 2008
Revised 5 March 2008
Accepted 31 March 2008

Abstract

Purpose – This paper aims to improve understanding of individuals' awareness and perceptions of computer usage policies (CUPs) and why individuals elect not to read these policies.

Design/methodology/approach – MBA students were asked to complete an online survey evaluating their behavioral intention to read CUPs, as well as their performance of this behavior. Factors contributing to the intention to read policies were also examined. The resulting data were analyzed with Smart PLS.

Findings – Results suggest that three factors influence individual intention to read CUPs. These factors include attitude, apathy, and social trust. The model explained about 70 percent of individual intention to read CUPs and about 44 percent of the variability in actually reading these policies.

Research limitations/implications – The sample is limited to MBA students from a single university.

Practical implications – Although written policy statements are often considered the cornerstone of computer security, many individuals elect not to read these policies. Thus, other methods of communication must be used.

Originality/value – This paper examines the reasons individuals elect not to read CUPs. Given the importance of these policies as deterrents to information systems misuse and computer crime, understanding why individuals fail to read policies is a critical first step in enhancing user knowledge of computer security.

Keywords Information systems, Crimes, Computers, Individual behaviour, Business policy

Paper type Research paper

Introduction

Information systems misuse and computer crime is a serious and ongoing problem. Although the cost and frequency of misuse and computer crimes seems to be declining (Gordon *et al.*, 2006), the problem still remains significant. One approach to computer security focuses upon the use of computer usage policies (CUPs), which are the cornerstone of computer security (Backhouse and Dhillon, 1995). These policies play an increasingly important role in organizations. Such policies have been used as an attempt to curtail employee access to material deemed inappropriate for the work

Industrial Management & Data Systems
Vol. 108 No. 6, 2008
pp. 701-712
© Emerald Group Publishing Limited
0263-5577
DOI 10.1108/02635570810883969

environment (Breakey, 2007), and violations of these policies have resulted in dismissal of employees (Brodwater, 2007). Recently CUPs have been identified as a communications issue between attorneys and clients, as the content and enforcement of such policies may impact attorney-client privilege (Lindquist, 2008). Unfortunately, despite the importance of CUPs, existing research suggests that many users do not read these policies (Foltz *et al.*, 2004).

Computer use policies

CUP defines who is allowed to use computer facilities and how those facilities may be used within an organization. The CUP is an organization's official position on computer use, and 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, and employee and employer rights. 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).

CUPs are expected to deter misuse by giving legal notice about expected use, by providing instructions in expected use, by explaining disciplinary actions, and by requiring acknowledgement. However, CUPs are only effective if they are read, understood, and obeyed.

Purpose

Since CUPs serve as the cornerstone of computer security (Backhouse and Dhillon, 1995), the tendency of individuals to not read such policies is of concern. 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 CUPs.

Literature review

Significant research regarding information systems security has been conducted over the years. For example, many authors have examined the frequency and cost of IS misuse and computer crime, while others have proposed methods and approaches to preventing misuse. Unfortunately, little research exploring why individuals elect not to read usage policies was found. However, human behavior research relevant to a decision to read CUPs does exist.

Frequency and cost of IS misuse and computer crime

The frequency and the cost of IS misuse and computer crime have often been evaluated. For example, an early estimate from the National Center for Computer Crime Data placed the annual cost at $555 million (Romney, 1995). Other authors have avoided placing specific dollar estimates on the cost of misuse, preferring instead to simply suggest that the annual cost of misuse is in the millions or billions of dollars (Straub and Nance, 1990). The frequency of misuse has also been evaluated. Specifically, 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). More recently, the CSI/FBI Computer Crime and Security Surveys have presented an annual measurement of both cost and frequency of misuse.

For example, the 2006 CSI/FBI Computer Crime and Security Survey reports that the frequency of successful attacks on systems has been declining since 2001, noting that only 52 percent of respondents reported unauthorized system use. Further, the 2006 CSI/FBI survey also notes that losses from IS misuse and computer crime are falling (2003 losses totaled $201,797,340, while 2006 losses totaled $52,494,290) (Gordon *et al.*, 2006). Although the reported decline in both frequency and costs seems to be good news, the frequently-cited CSI/FBI surveys are also subject to criticism from a number of sources. For example, the survey does not track respondents from year to year, so the trends reported may be inaccurate (Flickes, 2004). Other authors express concern over the CSI/FBI sample as well (Heiser, 2002). In addition, Flickes (2004) notes that the financial losses reported in the CSI/FBI survey do not match losses reported by other surveys (Flickes cites a US Secret Service survey which estimated annual losses of $666 million). Despite concerns with specific survey instruments and studies, 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

A number of computer security models (CSMs) have been developed to help cope with the threat of Information Systems Misuse and Computer Crime. 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 confidentiality, integrity, availability (CIA) framework; while others utilize behavioral or criminological theory. Still other research has focused on social theory (Lee and Lee, 2002). Although interesting, the CIA models are less applicable to the current study than are the behavioral and criminological theory models. These models all assume user familiarity with CUPs.

Straub's computer security model

Straub's Computer Security Model (Straub, 1986) is very relevant to the current research since it assumes that users are familiar with organizational CUPs. The CSM suggests the need for multiple layers of protection against misuse. These layers include deterrents, preventives, and detectives (Straub, 1986). Deterrents, which are based on the theory of general deterrence (TGD), are policies explaining acceptable and unacceptable uses of organizational information systems (Straub, 1986). Existing research suggests that deterrents reduce misuse in organizations (Klette, 1975; Straub, 1987). However, deterrents are primarily effective in blocking misuse perpetrated by insiders. Preventives consist of active measures such as passwords and encryption. These methods actively limit system and data access (Straub, 1986) and are effective at preventing misuse conducted by insiders and outsiders alike. Detectives, the final layer of the CSM, are 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 TGD. The idea of preventing unacceptable behavior such as crime by using the threat of punishment can be traced at least to Bentham in the eighteenth century (Nagin, 1978). Deterrence is "the preventive effect which actual or threatened punishment of offenders has upon potential offenders" (Buikhuisen, 1974, p. 285). 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.

The TGD assumes that individuals are fully aware of sanctions (Blumstein *et al.*, 1978). Existing research suggests that this is not true (Foltz *et al.*, 2004; Assembly Committee on Criminal Procedure (State of California), 1975). To understand human behavior in regards to reading or not reading CUPs, we should examine more fundamental behavior models, specifically the theory of planned behavior (TPB) (Ajzen, 1991) as well as social trust and apathy.

Approaches to understanding and predicting human behavior

This study focuses on the human behavior of reading, or not reading, computer usage policies. Entire disciplines, such as psychology, are devoted to understanding, explaining, and predicting human behavior. From these fields two theories were identified that are appropriate to this study. These theories, the TPB and social trust, both predict and explain human behavior. In addition, apathy is another variable which could help explain some of this behavior. The following is a brief synopsis of each of these areas.

Theory of planned behavior

The TPB suggests that the best way to predict an individual's behavior is by examining how that individual intends to behave. Behavior is also predicted by the individual's opinion about their ability to perform a behavior – people are less likely to attempt a behavior if they feel that performing the behavior will be difficult for them (Ajzen, 1988, 1991; Doll and Ajzen, 1992).

The TPB also explains how intentions are formed. Intentions are formed from three different variables, labeled attitude toward the behavior, subjective norm, and perceived behavioral control (Ajzen, 1991). Attitude toward the behavior reflects how an individual feels about performing the behavior (Ajzen, 1991). Subjective norm measures what the individual thinks others feel about the behavior (Ajzen, 1991) and could be likened to peer pressure. Finally, perceived behavioral control reflects the individual's opinion of their ability to perform the behavior. Perceived Behavioral Control includes the individual's perceptions of their own skills, abilities, emotions, compulsions, opportunity, and dependence upon others (Ajzen, 1988).

Recent research suggests that at least one of the TPB variables may vary over time. Leonard and Cronan (2005) examined the formation of attitude toward the behavior. The authors note that attitudes are formed from a variety of factors or attitude influencers, and that these attitude influencers are not permanent. For example, a period of prolonged media coverage was found to change attitudes toward the behavior of computer security (Leonard and Cronan, 2005).

The TPB variables may influence an individual's decision to read a computer usage policy. Individuals may have negative attitudes toward such policies, may perceive that others think everyone should read them, and/or may perceive the reading of such policies as difficult.

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 individual ability to perform a given behavior. However, individuals may substitute social trust for knowledge of risks associated with technology (Earle and Cvetkovich, 1995). Social trust is the willingness to rely on others who are responsible for making important decisions related to the management of technology, the environment, medicine, etc. especially when the individual lacks the interest, time, abilities, knowledge, or other resources to make decisions themselves (Siegrist *et al.*, 2000).

With the advent of the internet and collaborative technology the reality of an increasingly interconnected world has highlighted the need for a better understanding of social trust (Cook, 2001). As users become more dependent on technology and organizations provide increased access to these technologies, social trust may influence individual decisions to read organizational CUPs. If an organization provides well-trained individuals to cope with IS security threats, users may feel there is no need to invest limited personal time reading the policies, since other individuals are already responsible for protecting the system. Thus, some individuals may decide not to read the policies.

Apathy

Apathy is another possible determinant of intention and behavior of reading computer usage policies (Foltz *et al.*, 2007). Apathy has been identified as a 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, or may feel that the policies do not apply to them. Apathy is simply the lack of concern on the part of the user.

Research questions and conceptual model

The primary research questions of this study are:

RQ1. Do users elect to not read computer use policies?

RQ2. 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.

Methodology

Constructs and measurement

This study examines relationships among five possible determinants of intention to read computer use policies with intention and 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 scales adapted to reading computer usage policies. Intention was measured with Madden *et al.*'s (1992) and Beck and Ajzen's (1991) items. Behavior was measured using a ten-point Likert scale.

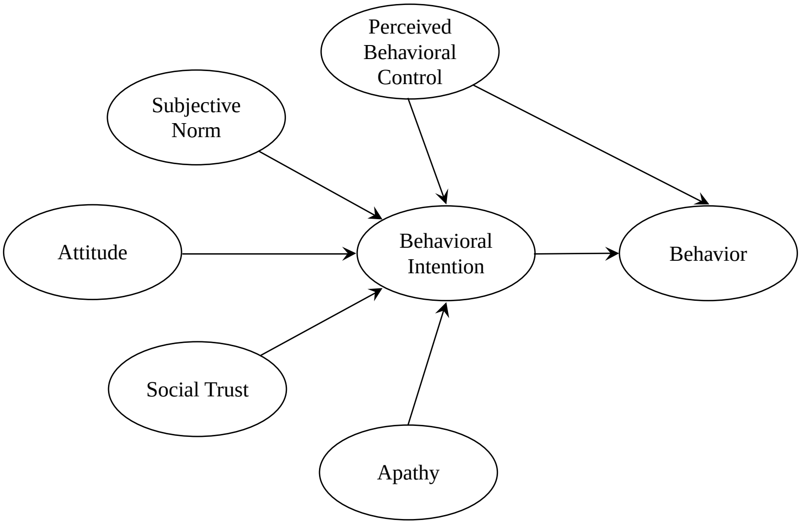


Figure 1.
Proposed model

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 *et al.* (2000) and Siegrist and Cvetkovich (2000). Apathy was operationalized by five questions measuring interest, emotions, and motivation on a five-point scale.

Data collection

Data for this study was collected utilizing a web-based survey administered to students in MBA classes. Students were from a variety of backgrounds with varying levels of experiences. Approximately half the respondents considered themselves fulltime working professionals.

At the start of the survey the MBA students were greeted by a short letter informing them that participation was voluntary and anonymous. At the end of the letter, students were presented with a text box for an access code. Students entered a set code to access the survey. Use of this code helped insure that only those asked to participate actually participated. The code was also useful in calculating the response rate.

Hypotheses

To answer the research questions posed earlier, a variety of hypothesis were tested:

H1. Perceived behavioral control will positively affect behavioral intention.

H2. Subjective norm will positively affect behavioral intention.

H3. Attitude will positively affect behavioral intention.

H4. Social trust will positively affect behavioral intention.

H5. Apathy will negatively affect behavioral intention.

H6. Behavioral intention will positively affect behavior.

H7. Perceived behavioral control will positively affect behavior.

Respondent characteristics

A variety of backgrounds and perspectives were represented by the respondents, who were all members of an MBA level course. Tables I and II present a summary of the respondent characteristics. Overall 171 responded with 86 indicating that they were fulltime working professionals and 80 indicating that they were fulltime students.

The respondents were evenly distributed by gender, represented a variety of ages, and years using computers. They considered themselves to be fairly knowledgeable about computers.

The professional respondents were well educated. Eleven had graduate or doctorate degrees. The professional respondents had an average of 8.26 years of industry experience in both small and large companies from a variety of industries.

Results

Results from this study are promising. An examination of the structural model using Smart PLS indicates that the model explains approximately 70 percent of the variability in behavior intention ($R^2 = 0.719$) and 44 percent of the variability in behavior ($R^2 = 0.439$). These results are based upon 171 responses from students enrolled in an MBA-level information systems class over several semesters (171 of approximately 200 students responded to the survey, for an 85 percent response rate). Further, a measurement model of the six main constructs was estimated using

< 20	0	Male	82	< 1	0	Very little	0
20-24	54	Female	89	1-3	26	Somewhat	0
25-29	61			3-5	80	Knowledgeable	3
30-39	39			5-10	52	Very	31
40-49	13			> 10	13	Extremely	139
50-59	4						
> 60	0						

Table I. Characteristics of all respondents

Education		Year in industry		No. of employees		Industry	
Associate	1	Min.	1	Min.	1	Agriculture/mining/construction	1
Bachelors	72	Max.	35	Max.	40000	Durable manufacturing	6
Graduate	8	Average	8.26	Average	17274	Finance/insurance/real estate	9
Doctorate	3					Food service	3
						Government	6
						Health care	15
						Information systems	8
						Non-durable manufacturing	2
						Services	9
						Trade and retail	8
						Transportation and public utilities	4
						Other	

Table II. Characteristics of business professional respondents

reflective indicators. Construct reliability was assessed using composite reliability. All but one of the construct reliabilities exceeded Nunnally's (1978) suggested 0.7 benchmark (social trust almost cleared the hurdle at 0.69). Convergent validity was examined using the average variance extracted measure. Intention, Behavior, and Subjective Norm cleared Fornell and Larcker's (1981) suggested 0.5 benchmark with scores of 0.59, 0.51, and 0.54, respectively. Unfortunately, four constructs fell short: Perceived Behavioral Control generated an AVE score of 0.41, while the scores for Apathy, Social Trust, and Attitude were 0.48, 0.32, and 0.26, respectively.

In addition, each of the seven hypotheses was examined using *t*-tests (170 degrees of freedom). Four of the hypotheses were supported, while three were not. *H3* is supported at the 0.001 level (*t*-value of 3.60, $\beta = 0.360$), suggesting that Attitude does influence Behavioral Intention. *H4* is supported at the 0.05 level (*t*-value = 1.74, $\beta = 0.099$), suggesting that Social Trust does influence Behavioral Intention. Also, *H5* is supported at the 0.001 level (*t*-value of 4.99, $\beta = -0.476$), suggesting that Apathy negatively affects Behavioral Intention. *H6* was also supported at the 0.001 level (*t*-value of 6.24, $\beta = 0.590$), suggesting that Behavioral Intention positively affects Behavior. *H1*, *H2*, and *H7* were not supported, suggesting that, in this situation, Perceived Behavioral Control and Subjective Norm do not influence Behavioral Intention (*H1* *t*-value of 0.046, $\beta = 0.004$, *H2* *t*-value of 0.509, $\beta = 0.034$), and Perceived Behavioral Control does not affect Behavior (*H7* *t*-value of 1.14, $\beta = 0.134$). The results are tabulated in Table III and shown in Figure 2.

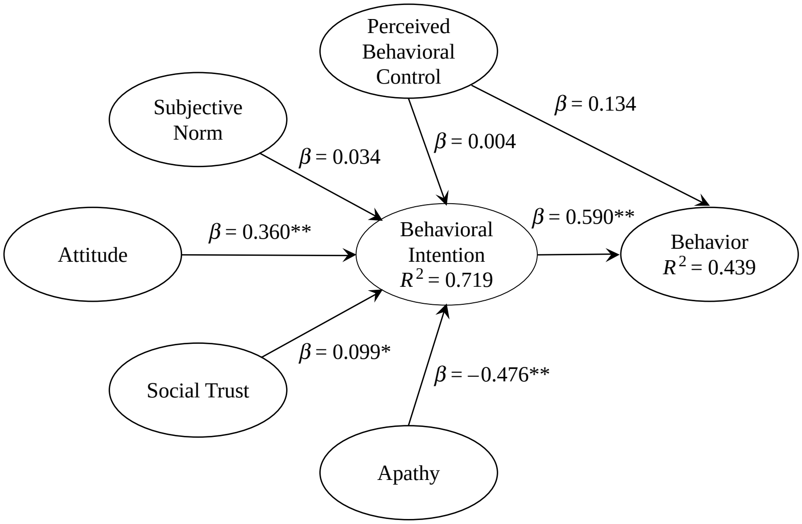
Discussion

The purpose of this research was to investigate why individuals elect not to read computer usage policies. The results of this study suggest that attitude, apathy, and social trust contribute to the formation of Intention to read computer use policies, while perceived behavioral control and subjective norm do not. Further, the research confirmed the positive relationship between intention and behavior and as such is a validation of the construct with past studies using the same variables (Vankatesh *et al.*, 2003).

Attitude and apathy have the greatest influence on intention to read CUPs. This suggests that individuals with positive opinions of CUPs are more likely to read them, while individuals who simply do not care (are apathetic) will not read them. Further, the small positive influence of Social Trust on Intention suggests that faith in others does contribute to this decision. Perhaps further research is needed to understand what role, if any, social trust plays in computer security.

Table III.
Results

Hypothesis	β-value	*t*-value	Level of significance
H1. Perceived control will positively affect behavioral intention	0.004	0.046	Not supported
H2. Subjective norm will positively affect behavioral intention	0.034	0.509	Not supported
H3. Attitude will positively affect behavioral intention	0.360	3.59	0.001
H4. Social trust will positively affect behavioral intention	0.099	1.74	0.05
H5. Apathy will negatively affect behavioral intention	−0.476	4.99	0.001
H6. Behavioral intention will positively affect behavior	0.590	6.24	0.001
H7. Perceived behavioral control will positively affect behavior	0.134	1.14	Not supported



Notes: *Significant at the 0.05 level; **significant at the 0.001 level

Figure 2.
Results

The larger impact of attitude and apathy on intention to read CUPs suggests that individuals tend to rely more upon internal factors – their own perceptions of the need to read computer usage policies – than on the influence or opinions of others (subjective norms). Perhaps these internal factors could be modified through a training and education program focusing on the importance of individual actions in guarding organizational computer security.

Although the TPB suggests that perceived behavioral control will influence intention and behavior, these relationships were not supported in the current study. This may be a reflection of our environment. Many organizations and universities utilize computer usage policies. Employees and students are not given an option – they are required to read (and abide by) these policies. There are simply no options, as failing to read the policies may prevent individuals from using information systems necessary for their own success. Thus, individuals may feel they have no option but to read (or to claim they have read) the CUPs. In addition, PBC focuses upon an individual's perceptions of their ability to perform an action – in this case, to read the CUPs. Respondents to this (written) survey are presumably all literate – thus, the lack of significance may reflect reality – all of the respondents could legitimately have felt able to read the computer usage policies.

The TPB also suggests that subjective norms will influence Intention. However, this relationship was not supported in the current study. This may also be a result of the environment – if everyone is required to read the CUP, there may be little discussion among individuals and referent others about the merits of reading the policies. Further, the results support a relationship between Apathy and Intention. Perhaps the apathy reported by individuals extends to referent others, or simply overrides the impact of referent others.

Conclusions and directions for future research

This research examines a model intended to explain why individuals elect to read computer usage policies. The model, while imperfect, explains almost 72 percent of the variance in the behavioral intention to read computer usage policies and almost 44 percent of the variance in actual behavior of reading such policies. This is a good result; 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. Other variables that might influence the reading of computer usage policies should be explored, such as the effect of voluntariness or overexposure, as well as specific characteristics of the computer usage policies. For example, the length and complexity of language used within these documents may induce user fatigue, causing some individuals to avoid reading the entire document. Also, since computer usage policies are relatively common, overexposure may cause users to forego reading them. Future studies should evaluate the length and complexity of computer usage policies, as well as pre-existing user exposure to such policies, to better distinguish between user apathy and fatigue.

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. A method for increasing the favorable attitude to reading such policies and overcoming the apathy toward reading them must be found.

In addition, the fact that social trust had some statistically significant, though small influence on the decision to read computer usage policies opens a new avenue for future research. How, and to what degree, does social trust influence Intention? Does reading a computer usage policy generate social trust? Does social trust lead users to abandon individual efforts to maintain organizational security? These questions must be addressed in future research.

References

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

Ajzen, I. (1991), "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, Vol. 50 No. 2, pp. 179-211.

Anthes, G.H. (1996), "Hack attack: cyberthieves siphon millions from US firms", *Computerworld*, Vol. 30 No. 16, p. 81.

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

Backhouse, J. and Dhillon, G. (1995), "Managing computer crime: a research outlook", *Computers and Security*, Vol. 14 No. 7, pp. 645-51.

Beck, L. and Ajzen, I. (1991), "Predicting dishonest actions using the theory of planned behavior", *Journal of Research in Personality*, Vol. 25 No. 3, pp. 285-301.

Blumstein, A., Cohen, J. and Nagin, D. (Eds) (1978), *Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates*, National Academy of Sciences, Washington, DC.

Breakey, P. (2007), "Delaware board sets computer-use policy", *Knight Ridder Tribune Business News*, October 11, available at: www.thedailystar.com/archivesearch/local_story_284040041.html (accessed April 4, 2008).

Brodwater, T. (2007), "Firefighters put on suspension: technician finds sexual images on Timberlake district's computers", *Knight Ridder Tribune Business News*, April 11, p. 1.

Buikhuisen, W. (1974), "General deterrence: research and theory", *Abstracts on Criminology and Penology*, Vol. 14 No. 3, pp. 285-8.

Cook, K.S. (Ed.) (2001), *Trust in Society*, Russell Sage Foundation, New York, NY.

Doll, J. and Ajzen, I. (1992), "Accessibility and stability of predictors in the theory of planned behavior", *Journal of Personality and Social Psychology*, Vol. 63 No. 5, pp. 754-64.

Earle, T. and Cvetkovich, G. (1995), *Social Trust: Toward a Cosmopolitan Society*, Praeger, Westport, CT.

Flickes, M. (2004), "Behind the numbers: the FBI cyber-crime survey results", Government Security web site, http://govtsecurity.com/mag/behind_numbers_fbi/ (accessed August 1, 2004).

Foltz, C.B., Anderson, J.E. and Schwager, P.H. (2007), "Factors influencing awareness of computer usage policies", *Proceedings of the Southwest Decision Sciences Institute, San Diego, CA*, pp. 243-52.

Foltz, C.B., Cronan, T.P. and Jones, T.W. (2004), "Student awareness of university computer usage policies: is a single exposure enough?", *Proceedings of the Southwest Decision Sciences Institute, Orlando, FL*, pp. 293-9.

Fornell, C. and Larcker, D. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 18, pp. 89-98.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Richardson, R. (2006), "2006 CSI/FBI computer crime and security survey", *Computer Security Journal*, Vol. 22 No. 3, pp. 1-21.

Heiser, J. (2002), "Go figure", *Information Security*, April, p. 26.

Holmes, J. (2003), "Formulating an effective computer use policy", *Information Strategy: The Executive's Journal*, Vol. 20 No. 1, pp. 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, M. and Tipton, H.F. (Eds) (1998), *Handbook of Information Security Management*, Auerbach, Boca Raton, FL.

Lee, J. and Lee, Y. (2002), "A holistic model of computer abuse within organizations", *Information Management & Computer Security*, Vol. 10 No. 2, pp. 57-63.

Leonard, L.N.K. and Cronan, T.P. (2005), "Attitude toward ethical behavior in computer use: a shifting model", *Industrial Management & Data Systems*, Vol. 105 No. 9, pp. 1150-71.

Lindquist, C.D. (2008), "Commentary: use of employer's e-mail in attorney-client communication raises privilege concerns", *Daily Record*, January 3, p. 1.

Madden, T.J., Ellen, P.S. and Ajzen, I. (1992), "A comparison of the theory of planned behavior and the theory of reasoned action", *Personality and Social Psychology Bulletin*, Vol. 18 No. 1, pp. 3-9.

Nagin, D. (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, DC, pp. 93-139.

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

Robert, P.H., Clairet, S., Benoit, M., Koutaich, J., Bertogliati, C., Tible, O., Caci, H., Borg, M., Brocker, P. and Bedoucha, P. (2002), "The apathy inventory: assessment of apathy and awareness in Alzheimer's disease, Parkinson's disease and mild cognitive impairment", *International Journal of Geriatric Psychiatry*, Vol. 17 No. 12, pp. 1099-105.

Romney, M. (1995), "Computer fraud – what can be done about it?", *The CPA Journal*, Vol. 65 No. 5, pp. 30-3.

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*, pp. 61-7.

Siegrist, M. (2000), "The influence of trust and perceptions of risks and benefits on the acceptance of gene technology", *Risk Analysis*, Vol. 20 No. 2, pp. 195-203.

Siegrist, M. and Cvetkovich, G. (2000), "Perception of hazards: the role of social trust and knowledge", *Risk Analysis*, Vol. 20 No. 5, pp. 713-9.

Siegrist, M., Cvetkovich, G. and Roth, C. (2000), "Salient value similarity, social trust, and risk/benefit perception", *Risk Analysis*, Vol. 20 No. 3, pp. 353-62.

Straub, D.W. (1986), "Deterring computer abuse: the effectiveness of deterrent countermeasures in the computer security environment", dissertation, Graduate School of Business, Indiana University, Bloomington, IN.

Straub, D.W. (1987), "Controlling computer abuse: an empirical study of effective security countermeasures", *Proceedings of the International Conference on Information Systems*, pp. 277-89.

Straub, D.W. and Nance, W.D. (1990), "Discovering and disciplining computer abuse in organizations: a field study", *MIS Quarterly*, Vol. 14 No. 1, pp. 45-60.

Taylor, S. and Todd, P.A. (1995), "Understanding information technology usage: a test of competing models", *Information Systems Research*, Vol. 6 No. 2, pp. 144-76.

Vankatesh, V., Morris, M., Davis, G. and Davis, F. (2003), "User acceptance of information technology: toward a unified view", *MIS Quarterly*, Vol. 27 No. 3, pp. 425-78.

Further reading

Haines, R. and Leonard, L.N.K. (2007), "Individual characteristics and ethical decision-making in an IT context", *Industrial Management & Data Systems*, Vol. 107 No. 1, pp. 5-20.

Corresponding author

C. Bryan Foltz can be contacted at: foltz@utm.edu