Appropriate Use of Information Systems:
A Policy Training Approach

Meagan E. Brock, College of Business, West Texas A & M University, Canyon, TX, USA

M. Ronald Buckley, Division of Management, University of Oklahoma, Norman, OK, USA

ABSTRACT

With the advancement of technology, there has been a commensurate increase in the use of information systems in American Universities. However, these increases have yielded an increase in both resource misuse and attacks on University information system networks. Data from 155 undergraduate students was used to investigate the role of policy presentation, on students' knowledge and transfer of information system policies. Results indicate that policy training does improve knowledge of information systems policies and transfer to novel situations however the form in which this training is presented is not important, as long as the information is presented in some format.

Keywords: *Checklist, Codes and Policies, Documentation, E-mail, Guidelines, Information Overload, Internet, Technoethics, Training*

INTRODUCTION

The advent of new technologies across the decades has ubiquitously created challenges for organizations of both the technical and ethical nature. For instance, information technology systems, more specifically the Internet and electronic mail (E-mail) are widespread and well-established tools for business and personal communications in organizations. However, with the introduction of new tools, so to has comes misuse of those tools, such as confidential file sharing music piracy, and internet-facilitated idea theft/ plagiarism to name a few. In attempt to research and understand how new developments in science and technology impact organizations and behavior, the field of technoethics was established (Bunge, 1977). Research in the area of technoethics goes beyond an understanding of how technology is created, maintained and utilized. Specifically, it explores the moral and ethical aspects of technology as they relate to society, in the hopes of creating a better understanding of systems and practices related to technology (Luppicini, 2010; Luppicini & Adell, R, 2008). There is currently an abundance of research detailing the use of information technologies and how to control and regulate practices of such resources in business settings (Aiello, 1993; Aiello & Kolb,

DOI: 10.4018/jte.2013010102

1995; Alge, Ballinger, & Green, 2004; Case & Young, 2002; Case & Young, 2001; Chen & Ross, 2005; Eddy, Stone, & Stone-Romero, 1999; Moula & Giavara, 1995). However, there exists scant research on the use and regulation of such technologies in higher education settings. In a private business setting the employer can secure, regulate, and monitor all information systems. Unlike the business sector, at a university there are issues with academic freedom and information exchange, rendering these systems more vulnerable to damage due to malicious attacks as well as to accidental damage from everyday heavy use and misuse (Olsen, 2002; Dignan, 2004). Thus, it is imperative to research how technoethics applies to university settings.

The vulnerability of universities is due to the fact that they cannot tightly monitor and control systems like can be done in business organizations. Further the nature of the educational environment is different than that of an organization. At a university one is likely paying to be there and administrators have very limited control over what you do. While in the workplace you are there to earn a paycheck with the primary purpose of organizational support. The uses of electronic information systems serve a critical function within universities and colleges by helping students, faculty, and colleagues exchange knowledge, ideas and information. These are fundamental elements of the mission of any college and university. Thus, both malicious and irresponsible use of these systems has the possibility of severely disrupting these vital functions.

Features which make the internet and e-mail so appealing (speed, interactivity, apparent privacy and impermanence) have resulted in negligence in computer communications, with the internet there is a loss in physicality and with that individuals may feel a lack of accountability (Anderson, 1996). "The threats, according to technology executives at universities, include the introduction of viruses into school networks, improper use of file sharing services, hogging bandwidth when downloading huge graphic files such as movies, and outright theft of information about their school records, those of other students and personal data that can be reused in online transactions" (Dignan, 2004, p. 13). Results from misuse can include system weakening or failure, lawsuits from illegal downloading, lawsuits regarding harassment, and disgruntled students, faculty, and administrators, to name a few. Due to the potential for disastrous results from information systems misconduct, policies regarding acceptable use of information resources, as well as techniques with which to monitor the systems have been implemented in colleges and universities. Universities have invested large sums of money on information systems for reasons discussed above, in order to curtail their weaknesses in the safeguarding of their systems (McClure, 2006).

While many universities do suffer from the occasional malicious security breach, other acts of misconduct are far more common and have the potential for a cumulative negative impact. Such acts include the misuse of e-mail resources, including spamming, forwarding, and harassment, misuse of campus computer facilities, and use of the campus network resources for downloading illegal materials. While illegal downloading has received much media attention and many universities have taken precautions in this regard, much more could be done in order to minimize threats to computer systems. For instance, a 2004 survey conducted by the research organization, Student Monitor, revealed that 29% of undergraduate students download illegal materials, and 75% of undergraduate students believe that such downloading should be made legal (Angelo, 2005). Thus, it can be assumed that currently implemented programs regarding downloading are ineffective.

Recently, it has been suggested that many of the "attacks" on computer networks by students are often accidental and not malicious in nature (McCollum, 1998). An example of an accidental attack is opening and/or forwarding an e-mail that carries a virus, resulting in harm to the universities network and those who access it. These accidental "attacks" on university networks may be due to a lack of understanding of information systems policies, and the consequences of violating these policies. Therefore, educational