8-2008

An Analysis of Perceived Faculty and Staff Ccomputing Behaviors That Protect or Expose Them or Others to Information Security Attacks.

Chiwaraidzo Judith Nyabando
East Tennessee State University

An Analysis of Perceived Faculty and Staff Computing Behaviors that Protect or Expose Them or Others to Information Security Attacks

---

A dissertation

presented to

the faculty of the Educational Leadership and Policy Analysis Department

East Tennessee State University

In partial fulfillment

of the requirements for the degree

Doctor of Education

---

by

Chiwaraidzo Judith Nyabando

August 2008

Dr. Jasmine Renner, Chair

Dr. James Lampley

Dr. Phil Pfeiffer

Dr. Terry Tollefson

Keywords: information security, faculty and staff, mixed-methods research, information technology

ABSTRACT

An Analysis of Perceived Faculty and Staff Computing Behaviors that Protect or Expose Them or Others to Information Security Attacks

by

Chiwaraidzo Judith Nyabando

A mixed-methods study, conducted in 2007-2008, designed to quantify and assess behaviors that either protect or expose data at academic institutions to information security attacks. This study focused on computing practices at two academic institutions: East Tennessee State University and Milligan College. Interviews with six information technology professionals and online surveys were used to assess faculty and staff members' awareness and practice of safe computing behaviors. The constant comparison method was used to analyze qualitative data. Descriptive statistics and univariate and multivariate analysis of variance techniques were used to analyze the quantitative data.

Overall, the analyses indicated that the faculty and staff members at these institutions were equally aware of information security issues and practices and tended to practice safe computing behaviors—though apparently at a level that was less than commensurate with their awareness of these behaviors. Raised awareness correlated with safe computing behaviors, as did computer usage: those who had used computers for more than 20 years appeared to be more aware of safe practice than those who had used computers for 20 years or less. Password management emerged as a major challenge for the participants. They were also concerned with phishing emails and they tended not to be aware of FERPA regulations.

DEDICATION

This dissertation is dedicated to God who made it possible for me to reach this milestone. I also dedicate this work to my parents, Lovemore and Matilda Nyabando, who made education a priority in our lives; to my aunts and uncles who supported my educational goals; to my brothers and sisters who encouraged me; and to my professors and mentors who taught and encouraged me.

ACKNOWLEDGEMENTS

My sincere gratitude and appreciation goes to my dissertation committee for guiding me through this process. Dr. Jasmine Renner, thank you for your constant support, encouragement, and advice. Dr. James Lampley, thank you for teaching me the art of research and for your encouragement. Dr. Phil Pfeiffer, thank you for your advice and support. Dr. Terry Tollefson, thank you for your generosity and support. All of you make ETSU a great place to explore knowledge.

I would also like to thank Mark Bragg, ETSU Associate Vice-President of Information Technology; Dr. Mark Matson, Milligan College Vice-President for Academic Affairs and Academic Dean; and Mark Nester, Milligan College Information Technology Manager, for assisting me.

Also, special thanks to Dr. Evelyn Roach, my auditor, and Dr. George Naholi, my peer debriefer, for checking the consistency of my work.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

Figure Page

CHAPTER 1

INTRODUCTION

Computer technology has allowed information to be shared to an unprecedented degree at a cost of making that information more susceptible to attack. In particular, computer networks like the Internet provide convenient access to information as well as a convenient point of attack for service disruption and information theft (Conklin, White, Cothren, Williams, & Davis, 2004).

Colleges and universities are at special risk for information theft. A study of 36 colleges and universities in the United States found that those institutions had suffered 319 attacks on their information resources (Young, 2005). In a study conducted in 2006 on information security in higher education, 124 of 182 participants indicated that their institutions had experienced at least one information security breach in 2005 (CDW Government). In June 2003 a computer virus at Stanford University broadcasted confidential employee salary and bonus information to about 35,000 Stanford users (Kvavik et al., 2003). In February 2003, an intruder accessed names and social security numbers of 59,000 students, faculty, and staff at the University of Texas at Austin (Kvavik et al.).

Although developers and researchers have provided ways to secure computer networks, authorized users can engage in practices that expose their host systems to attack. Bishop (2005) said "the heart of any security system is people" (p. 19). Users who are uninformed about and indifferent to information security problems tend to act in ways that increase the risk of security breaches and attacks, while users who are aware of these problems can, by implementing protective measures, help to prevent their occurrence.

Statement of the Problem

Colleges and universities are entrusted with confidential information about their students, alumni, employees, and other clients. Institutions of higher education must protect this information because the cost of insecurity can be very high (Foster, 2004). As a part of this

obligation, colleges and universities must continually assess their security status.

This study was undertaken in order to further the academic community's understanding of the potential risks to information security posed by employees of academic institutions. To this end, it sought to assess how faculty and staff at two institutions of higher learning—a public regional university (East Tennessee State University (ETSU)) and a private college (Milligan College)—do standard, computer-related tasks that impact data security: i.e. manage passwords, dispose of data storage devices and documents, back-up data, comply with the Family Education Records and Privacy Act (FERPA), contend with malware, and manage phishing e-mails. It was designed to assess faculty and staff members' awareness of information security practice as well as their behaviors.

Research Questions

For the purpose of this study, these goals were framed in terms of the following five research questions:

1. What are the computing behaviors of faculty and staff members that can either protect or expose them or others to information security attacks as observed by information technology professionals?
2. What are the faculty and staff members' attitudes toward the role they play in securing computer systems as reported by the faculty and staff members?
3. What are the faculty and staff members computing behaviors reported by the faculty and staff members that either protect or expose them or others to information security attacks?
4. In what ways, if any, do attitudes towards information security, awareness of information security issues, and awareness of information security policies make a difference in how faculty and staff members use information technology?
5. What differences, if any, exist in information security awareness and practice among faculty and staff members with different demographic characteristics?

Significance of the Study

Smith (2004) states that risk assessment is the first step in creating an information security policy. Identifying faculty and staff computing behaviors that render academic institutions either more or less vulnerable to information security attacks and assessing the prevalence of these computing behaviors is a reasonable first step towards helping institutions like ETSU and Milligan College to evaluate their training programs and user policies in order to protect their information resources and its people from preventable attacks.

Delimitations and Limitations

The study was delimited to the faculty and staff at ETSU and Milligan. No attempt was made to determine the study's external validity: i.e. the extent to which its findings can be generalized to other institutions of higher education. Even so, it is hoped that these findings can help other institutions assess their information security needs and to develop effective programs for educating faculty and staff members on how to protect their information and that of their institution.

In order to address possible biases resulting from the author's concerns about information security, the study was designed to determine how different kinds of practices, both good and bad, affect institutional security in positive as well as negative ways.

Definition and Explanation of Terms

For the purpose of this study the following definitions will apply:

A computer system includes hardware, software, policies and procedures (Bishop, 2005).

Authorized users are people who have authorized access to certain information and resources (Conklin et al., 2004).

Dumpster diving occurs when an intruder searches trash for confidential information (Conklin et al., 2004) such as social security numbers and passwords.

Information security is the deliberate use of policies and practices to ensure the

confidentiality, integrity, availability, and proper use of information and information resources, as well as individual accountability for the use of those resources (Bishop, 2005; Conklin et al., 2004).

Information confidentiality refers to the secrecy of information (Bishop, 2005). Only individuals authorized to view certain information should have access to that information.

Information integrity refers to the trustworthiness of information (Bishop, 2005). "It is the accuracy, consistency and reliability of the information content, processes and systems" ("Information Integrity Defined", n.d.).

Information availability is the assurance that information is available and accessible when an authorized user needs to access it (Conklin et al., 2004). It is the assurance that an authorized user can access information without undue interruption.

Information nonrepudiation refers to the ability to verify that information was sent by the intended sender and received by the intended receiver; such that the sender cannot refuse having sent the information and the receiver cannot refuse having received the information (Conklin et al., 2004). Nonrepudiation equates to holding individuals accountable for their use of information and information resources (Conklin et al.).

Intruders, hackers, and unauthorized users are people who seek to gain access to information and resources they are not authorized to access (Conklin et al., 2004).

USB flash drive, also known as JumpDrive, is a removable data storage device that has a universal serial bus (USB) connector (Wikipedia, n.d.). It uses flash memory technology for general data storage and transfer (Wikipedia).

Malicious code or malware is software that is designed for a malevolent purpose (Conklin et al., 2004). Viruses, worms, Trojan horses, keystroke loggers, and spyware are examples of malware.

Social engineering is when an intruder manipulates an authorized user into disclosing confidential information (Conklin et al., 2004) such as a username or a password.

Phishing is a form of social engineering that involves "an attempt by a third party to

solicit confidential information from an individual, group, or organization, usually for financial gain" (Symantec, 2007, p 64). Phishing typically involves deception in the form of the attacker's masquerading as a legitimate entity who is seeking this information for supposedly legitimate purposes.

Shoulder surfing is when an intruder observes an authorized user as the user enters confidential information or observe the user's actions in order to get confidential information (Conklin et al., 2004).

Spoofing is when an entity assumes the identity of another, usually a trusted entity. (Conklin et al., 2004).

Vulnerabilities are weaknesses in computer systems that can be exploited by unauthorized users to gain access to the computer systems (Canavan, 2001). They are a result of flaws in the design, implementation, or operation of a computer system (Bishop, 2005).

Overview of the Study

The balance of this study is organized into four chapters. Chapter 2 reviews relevant work and background material, including the history of information security issues, information security, information security best practices and human and organizational behavior. The remaining three chapters present the study's methodology; data; and findings, conclusions, and recommendations.

CHAPTER 2

REVIEW OF LITERATURE

Chapter 2 reviews related literature on information security. Bishop lists three goals for information security: the prevention of attacks and unauthorized access to information; the detection of actual intrusions, and the maintenance of business continuity in the face of attacks, including recovery from those attacks (2005).

The review, which is organized into eight sections, begins with a discussion of information security issues from the 1960s to the present. The next three sections present theories of human behavior in relation to information technology, organizational culture issues in relation to information security, and information security attacks through an authorized user. The following three sections discuss the higher education computing environment, information security incidents involving institutions of higher education, and information security policies of ETSU and Milligan College, the institutions under study. The last section discusses best practices in information security.

Information Security from 1960 to the Present

From the early 1960s through the mid-1980s, information security efforts focused primarily on securing data on individual computer systems. Most of these systems were mainframes, which are very large and expensive computers, and minicomputers, which were midrange between mainframes and personal computers (Canavan, 2001). Most of these computers were not connected to a network. Data were processed and stored on a central computer and users interfaced with the computer through terminals (Bosworth & Jacobson, 2002). The terminals were not used to download and save data. The computers were accessible only to trained technicians (Bosworth & Jacobson). They were not available to the general public. Security concerns during this period focused on securing physical access to computers and securing operating systems (Canavan).

The first major computer network, the Advanced Research Projects Agency Network (ARPANET), was introduced in 1969 (Bosworth & Jacobson, 2002). The ARPANET, which was sponsored by the Department of Defense, connected research computers at University of California at Los Angeles, University of California at Santa Barbara, Stanford Research Institute, and University of Utah. This network was the predecessor to the Internet.

The ARPANET was the proving ground for TCP/IP, a set of procedures and standards that support reliable communication between heterogeneous computers (Canavan, 2001). TCP/IP, like the Internet, was made available to the public during the 1970s and 1980s (Canavan). These developments, along with the introduction of personal computers, affordable local area networking, and the development of new applications, introduced a new era of information technology. These technologies linked computer networks to the outside world. Programs could be executed on local computers, data could be transferred from one computer to another, and data could be stored on portable devices such as disks (Bosworth & Jacobson, 2002). Computer costs decreased and computers became available to the general public.

The popularization of computing also introduced a new wave of information security concerns. The severity of preexisting problems such as software vulnerabilities and malware was exacerbated by exposing systems to the Internet. New issues such as copyright infringement, online fraud, and identity theft emerged (Bosworth & Jacobson, 2002). Computer users grew from trained technicians to include non-technical people. The number of intruders also increased. In response to these threats, the literature on best practices in information security has broadened to encompass organizational and human factors, networks, and networking technologies (Trcek, Trobec, Pavesic, & Tasic, 2007).

The earliest documented attack on a computer network occurred in 1970, when an unknown individual released the Creeper virus onto the ARPANET (Elliott, Young, Collins, Frawley, & Temares, 1991). That virus, though harmless, spread through modems from one computer to another and displayed on the infected computers the message ‘I’M THE CREEPER: CATCH ME IF YOU CAN’ (Wikipedia, n.d.).

The first major attack on a computer network was the Morris worm of 1988. The worm was released by Robert T. Morris, a graduate student at Cornell University and the son of the former chief scientist at the National Computer Center, a branch of the National Security Agency (Rosenberg, 2004). The worm shut down about 6,000 computer systems by reproducing so rapidly that the computers had no time left to do any useful work (Conklin et al., 2004). That attack caused an estimated damage of about $100 million dollars (Conklin et al.).

Major attacks involving computer networks became more common following the Morris worm. These attacks have included attacks on networks, like the Melissa virus ($80 million in damages), the Love Letter worm ($10 million), and the Slammer worm of 2003 (Conklin et al., 2004). The Slammer worm infected over 120, 000 computers within the first 24 hours of its release, causing networks to go down and creating problems with ATMs and airline flights (Conklin et al.). At the University of Texas at Austin, 5,000 computers were infected by Slammer (Kvavik et al., 2003). Attacks on computers have also included unauthorized break-ins to computer systems like the Citibank and Vladimir Levin incident, wherein Levin stole $10 million by hacking Citibank's cash management system (Conklin et al.).

Studies by Symantec and others have indicated that network-based threats continue to challenge information security. Over a course of over 10 years that ended December 2006, Symantec (2007) identified about 20,000 system vulnerabilities. They also reported a 12% increase in vulnerabilities between July and December 2006 (Symantec). During the last half of 2006, their Symantec Probe Network received an average of 904 unique phishing messages per day. In addition, 66% percent of the top 50 malicious codes reported to Symantec between July 2006 and December 2006 were designed to expose confidential information.

Fifty-four percent of identity-theft-related attacks reported between July 2006 and December 2006 involved theft or loss of computers and storage devices (Symantec, 2007). A May 2006 incident involving a stolen U.S. Department of Veterans Affairs (VA) illustrates the potential severity of this risk. The VA discovered that a laptop computer that contained insurance claim information for millions of VA patients had been stolen from the home of one of its

employees (“Latest Information”, n.d.). The data on the laptop included patient names, dates of birth, and social security numbers (“Latest Information”).

Another issue that is currently of concern is unprotected wireless networks. Most home and public wireless access points are not protected, making it easier for intruders to intercept and access wireless communications (Barile, 2006). Most authorized users are not aware of the need to protect their wireless networks or how to protect them (Barile).

Analyses of information security incidents show that people attack computers for different reasons. Some people attack systems in order to assert their self-proclaimed right to access any information they want (Rosenberg, 2004). These individuals argue that

> [t]he very concept of secret information is offensive and that if it were not collected, there would be no need to protect it. Thus, they claim that their role must be to “liberate” the data, to defeat the notion of secure systems, and thereby to inhibit open-ended collection of information (Rosenberg, p 449).

Others, known as script kiddies, hack for the thrill of doing so. Script kiddies lack the technological skills to develop harmful programs or discover new vulnerabilities but are skilled enough to download and release harmful programs (Conklin et al., 2004). At the other end of the thrill-seeking spectrum one finds elite hackers: people who discover vulnerabilities and write harmful programs to manipulate them (Conklin et al.).

Still others, criminal groups and terrorists, are usually organized and supported by funding (Conklin et al., 2004). They are involved in criminal activities such as extortion, theft, forgery, fraud, and terrorism (Conklin et al.).

Human Behavior and Information Technology

Theories have been developed to explain human behavior towards technology. One such theory, Theory of Reasoned Action (TRA), asserts that behavior results from intentions that are produced by a person’s attitude toward that behavior and related subjective norms (Fishbein & Ajzen, 1975). A person’s attitude towards a behavior is a result of the person’s beliefs about the

behavior. Subjective norms are influences from other people in the person's social environment (Fishbein & Ajzen).

A theory more specific to information technology is the Technology Acceptance Model (TAM) (Davis, 1986). Davis, who adapted TAM from TRA, identified and specified two attitudes that influence user technology acceptance: perceived usefulness and perceived ease of use. Perceived usefulness has a greater influence than perceived ease of use because users are willing to accept a useful technology even though it may be a little difficult to use (Davis, 1989). Perceptions may change with time and perceived ease of use may increase as technologies become more widely used (as cited in Dillon & Morris, 1996).

Studies that validate TRA and TAM include Davis, Bagozzi, and Warshaw's comparative study of TAM and TRA (1989), Taylor and Todd's comparative study of IT usage by experienced and inexperienced users (1995), and Shih's user e-shopping acceptance study (2004).

Organizational Culture

Information security management, according to Anderson (2001), is an iterative process: a cycle of incidents and responses, including investitures in preventative measures (Anderson). Anderson argues that organizations can become complacent over time, reacting only when an incident occurs.

Aytes and Connolly (2004) attempted to document student computing behaviors at two large U.S. universities. Most participants indicated that they were aware of and knew how to protect themselves from information security problems. For example 69% indicated that they knew how to protect themselves against viruses and 50% indicated that they knew how to protect their financial information. However, 47% of those participants also indicated that they had never received any educational information about information security. Of those who had received information, it was from friends and colleagues and personal experience.

Some studies have shown that authorized users are becoming more aware of information

security threats and how to protect themselves because of the publicity given to information security incidents (Furnell, 2005). Most users have heard of viruses, worms, spyware, and phishing. This awareness helps users understand the importance of securing information systems (Furnell).

Additionally, Aytes and Connolly (2004) and Bishop (2005) state that users and organizations could be overconfident about security. Security policies could be implemented incorrectly, thereby giving a false sense of security (Bishop). Aytes and Connolly found that users who were aware of potential information security threats routinely thought that they were least likely to experience those attack themselves.

Avenues of Attack Through an Authorized User

Some security breaches involve deliberate theft or misuse of information resources by authorized users. This study, however, focuses on incidents where attackers exploit vulnerabilities that are created unintentionally by authorized users. Common avenues of attack through authorized users include weak passwords, shoulder surfing, dumpster diving, file sharing, social engineering, failure to log off after using a computer, and failure to backup files (Conklin et al., 2004).

Weak passwords are passwords that are too short, easy to guess, or never changed (Canavan, 2001). In 2003 the University of Pennsylvania identified weak passwords to systems as its major security problem (Foster, 2004). Users usually select passwords they can easily remember. The problem with many easy-to-remember passwords is that they can easily be reconstructed (Conklin et al., 2004).

Shoulder surfing involves the use of visual surveillance to obtain information to which a person is not entitled. Typically, the intruder positions herself or himself in such a way that an authorized user can be observed entering a password or other sensitive content (Conklin et al., 2004). Additionally, computer hardware devices emit electromagnetic radiation as they communicate with other peripheral devices (Stewart, Tittel, & Chapple, 2005). These

emanations can be intercepted by intruders to capture whatever is displayed on a monitor or typed on a keyboard (Stewart et al.).

Users routinely share files with one another on a daily basis, using e-mail attachments and portable storage devices such as flash drives. This sharing enables malware to be distributed through computer networks easily.

Social engineering is the manipulation of authorized users to disclose privileged information. According to Conklin et al. (2004), social engineers often exploit people's desire to help others. A classic example of a social engineer is Kevin Mitnick, who used impersonation to obtain confidential information such as passwords to accounts and files and names of key security officials (as cited in Rosenberg, 2004). He used this information to penetrate telephone company systems, steal files, and alter and move confidential files (Rosenberg). Mitnick hacked information systems from about 1989 to 1999, when he was eventually arrested (Rosenberg). Mitnick became a security consultant upon completing his sentence (as cited in Rosenberg).

Failure to log off after using a system provides an easy access to intruders. Failure to backup files is also a threat because if files become corrupted or are destroyed the information stored will be completely lost.

The Higher Education Computing Environment

Universities and colleges collect, store, and transact large amounts of private information about their students, employees, prospective students, alumni, and others connected to the institutions (Cate, 2006). The information includes student records, financial records, health records, academic records (Cate), and intellectual property. Institutions of higher education must also comply with Federal and State privacy and data protection laws.

Technology

A report compiled by Hawkins and Rudy (2006) for EDUCAUSE found that most of the 933 reporting colleges and universities used electronic technologies for data management. This

included course management systems such as Blackboard and multimedia classrooms with technologies such as wired Internet access, LCD projectors, computers, and smart boards. Most of the 204 institutions that participated in a study by Caruso (2006) had acceptable use polices for technology. Most institutions used VPN for remote network access (Caruso; Hawkins & Rudy). Most campuses were providing wireless Internet access (Hawkins & Rudy). Most employees had university e-mail accounts (Hawkins & Rudy).

Federal and State laws

The laws with which educational institutions need to comply include FERPA; the Health Insurance Portability & Accountability Act (HIPAA); the Electronics Communications Privacy Act (ECPA); the Patriot Act (Corkin et al, 2004); the Technology, Education, and Copyright Harmonization Act (TEACH); and various state laws that govern information technology in higher education (Salomon, Cassart, & Thibeau, 2003).

FERPA is a federal law established to protect the privacy of student records (U.S. Department of Education, 2006). FERPA applies to educational institutions that receive federal funds. Under FERPA, educational institutions must obtain written permission from the student or the parent before release any information in a student record. However, educational institutions can release directory information such as names, addresses, telephone numbers, and dates of birth without student or parental consent (U.S. Department of Education).

Virtually all educational institutions store some, if not all, student records in electronic form. This practice dramatically increases the amount of data covered by FERPA (Salomon, Cassat, & Thibeau, 2003). Institutions of higher education should have guidelines for how and where to store student information and how to secure this information such that only authorized users can view it. They also need to have FERPA-compliant procedures for processing student or parental requests for student records. Faculty, staff, students, and parents need to be informed about these procedures.

HIPAA was established to protect the privacy rights of patients. HIPPA standardizes the

transmission of electronic patient records, requires health providers to adopt written privacy policies and procedures that govern access to patient information, and requires the training of employees in protecting patient information privacy and the designation of a specific person(s) for ensuring that policies and procedures are followed in compliance with the law (Salomon et al., 2003). In 2000 the U. S. Department of Health and Human Services mandated that consumers receive written notices of the information practices of health care providers and other covered entities under HIPAA (Salomon et al.). These entities include institutions of higher education that are affiliated with health care providers (Salomon et al.).

The ECPA prohibits unauthorized use or interception of contents of any wire, oral, or electronic communication (Salomon et al, 2003). The law was established to protect workplace privacy and discourage unauthorized access to electronic resources (Corkin et al, 2004). ECPA prohibits employers and other organizations from monitoring computer usage without users' consent (Corkin et al). However, organizations have a right to protect their resources and in many cases that includes monitoring the activities of those using their networks. For this reason many organizations issue warnings that a user, by accessing these resources, gives the organization permission to monitor the user's activities on the organization's network (Corkin et al).

The PATRIOT Act amends the Foreign Intelligence Surveillance Act (FISA), FEPA, and ECPA among others (Jaeger, McClure, Bertot, & Snead, 2004). The Act, passed in the wake of 9/11 terrorist attacks, gives the FBI and other law enforcement agencies more latitude in conducting investigations.

At least two provisions of the PATRIOT Act affect institutions of higher education. The first allows law enforcement agents to request any library records of library patrons suspected of terrorist activities without the patrons' knowledge or consent (Jaeger et al, 2004). The second provision requires colleges and universities to submit personal information for all international students enrolled at their institutions to the Student Exchange and Visitor Information System (SEVIS) (Holub, 2003). SEVIS is a database of information on all international students enrolled

in United States colleges and universities (Holub).

The TEACH Act of November 2002 relaxes copyright laws in ways that enable accredited not-for-profit educational institutions and government bodies to use copyright-protected materials in distance education (Holub, 2003). Before TEACH was enacted it was difficult for instructors and students to share materials through the Internet and other digital media without violating copyright laws (Crews, 2006). TEACH allows instructors and students to share portions, not full text or lengthy copyrighted materials, through instructional technology within the context of a course (Crews).

TEACH enables educational institutions to establish copyright polices and guidelines regarding distance education at the institutions (Crews, 2006). The policies define standards for instructors to follow when using copyright materials. TEACH also makes institutions responsible for bringing awareness of the law and the guidelines to their faculty, student, and staff (Crews). Technology administrators on colleges and universities need to help ensure that access to these copyrighted materials is limited to students enrolled in that particular class only.

State authorities have established laws that affect the management of information resources by colleges and universities. These include data-breach disclosure laws that require victims to be notified if their private information is disclosed to unauthorized users (Foster, 2005).

Incidents on University Campuses

According to Kvavik et al. (2003), large institutions and doctoral institutions report far more attacks on their information resources than smaller institutions. For example, in June 2003 a computer virus at Stanford University broadcast confidential employee salary and bonus information to about 35,000 users at the university (Kvavik et al.). In February 2003, an intruder accessed names and social security numbers of 59,000 University of Texas at Austin students, faculty, and staff (Kvavik et al.). The University of Pennsylvania spent $287,000 in staff time to repair the damage incurred by the Blaster worm in 2003 (Foster, 2004). On December 12, 2006,

UCLA announced that an intruder, over the course of a year, had accessed a database that has personal information about UCLA students (current and former), faculty, and staff (UCLA, 2006). It is believed that the intruder had access to information on about 800,000 people.

About 30% of the institutions that Kvavik et al. (2003) surveyed had awareness programs on information security. Kvalik et al. found that the number of information security breaches increased as the number of information technology devices increased and as the number of users increased. In another survey of information technology officials, 41% of study participants reported that intruders had penetrated their systems during the previous year (Foster, 2004). According to Symantec (2007), the education sector accounted for 20% of all reported data breaches that could lead to identity theft during the July 2006 to December 2006 period, second only to the government sector, which experienced 25% of the breaches.

Studies by Ashe (2004) and Simons (2005) argue that higher education institutions make easy targets for attacks. Ashe and Simons attribute these vulnerabilities to a combination of decentralized information systems, a constant flow of new technologies, and a relative lack of personnel resources and administrative support to secure their information resources. Control over academic systems tends to be decentralized due to individual academic entities preferring to have control over resources to allow for an unrestricted learning environment. These systems are sometimes managed by users who have limited knowledge about how to set up and use the systems in a correct and secure manner. For example, Simons reported that 15 of the administrative accounts in the study had weak passwords or no passwords at all. This opens the door for attacks. Limited resources and limited administrative support presents a challenge in accounting for all available information resources and in eradicating known vulnerabilities (Ashe; Simons).

Information Security Policies at Institutions under Study

ETSU publishes two documents that define policies for using information technology resources. The first, the Information Technology Code of Ethics ("Information Technology Code

of Ethics", 2006), presents overall guidelines for faculty and staff usage. The second, ETSU's Acceptable Use Policy, mainly covers Internet use and publishing websites ("Acceptable Use Policy", 2000). Both documents specify the rights and responsibilities of persons authorized to access information technology resources. Both documents state that users are accountable for any activities that occur in his or her computer account, knowingly or unknowingly.

ETSU maintains information about virus protection and virus protection resources as well as online security awareness training ("Office of Information Technology", n.d.). This training is only for authorized ETSU users. ETSU's OIT also has an alerts section on its website where notices and alerts regarding information security are posted and updated regularly.

Milligan College's Computer Use Policy gives guidelines for computer use at Milligan College. The policy is intended for all faculty, staff, and students who use Milligan's computing resources ("Milligan College Computer Use Policy", n.d.). The policy describes an authorized user's responsibilities, gives examples of unacceptable actions, and describes the consequences of violating the policy's requirements.

Milligan College's information technology office maintains other resources on computer use for Milligan's faculty. These include instructions on how to back-up files and how to password-protect a computer when not in use, as well as links to sites for downloading anti-spyware software ("Information Technology", n.d.).

Best Practices

An information security policy is a recommended starting point for managing information security (Anderson, 2001; Bishop, 2005; Conklin et al., 2004). Thomson and Solms (2005) said that a policy's purpose "is to influence and determine decisions, actions and other issues, by specifying what behavior is acceptable and what behavior is unacceptable" (p. 71). A well-written policy can guide users in using the organization's resources securely. It should also outline users' responsibilities and give guidelines for acceptable use of resources.

Conklin et al. (2004) view policy implementation as a four-step process. In the first,

planning step, an organization identifies its assets and creates policies for managing risks to those assets (Smith, 2004). Next, the organization implements the policies, educating its users about the policies' requirements. The implementation should then be monitored and, finally, evaluated for effectiveness. Based on the evaluation's results, the policies can be adjusted, restarting the cycle. This is a continuous process because organizations and the environment surrounding them are always changing, and new threats continue to come.

Information security policies can include an acceptable use policy, an Internet usage policy, an e-mail usage policy, a disposal policy, a password policy, and anti-social engineering guidelines (Conklin et al., 2004).

An acceptable use policy outlines the proper use of an organization's information technology resources. It also outlines what a user may and may not do while using these resources.

The Internet usage policy specifically outlines what an organization's users may and may not do on the Internet while using the organization's resources. It should also specify procedures for posting materials on the Internet.

Related to the Internet usage policy is the e-mail usage policy. An e-mail usage policy explains what employees are allowed to send using the organization's e-mail resources. Employees should be aware that e-mail messages sent over the Internet, unless encrypted, can be read by anyone who intercepts the messages.

According to Conklin et al. (2004) intruders search for confidential information in discarded records and electronic media, including documents, letters, scratch paper, and old hard drives (Conklin et al.). These vulnerabilities should be addressed with polices for secure disposal of sensitive materials. Documents should be shredded into small pieces or should be burned to prevent reconstruction of information (Kissel, Scholl, Skolochenko, & Li, 2006). Data on unwanted electronic storage devices should be magnetically destroyed and the devices should be pulverized (Kissel, et al.).

A password management policy specifies guidelines for managing passwords. These

include policies for what passwords can be selected, how often passwords must be changed, and how to help users recover from forgotten passwords.

Passwords are the most widely used technique of verifying user identity (Canavan, 2001). Strong password policies—policies that require users to choose hard-to-guess passwords—are important for protecting systems against unauthorized access. The use of personal data as a password should be discouraged because anyone who can discover a user's personal information could guess these passwords (Conklin et al.). Examples of bad passwords based on personal data include birthdays, social security numbers, and names of relatives.

The characters that make up a user's password can also affect a password's strength. Conklin et al. (2004) also recommend against the use of letters-only passwords, as being too easy to guess. Various authorities recommend selecting passwords that are a combination of letters, numbers, and punctuation marks (Anderson, 2001; Canavan, 2001; Conklin et al.). Canavan also suggests that a password be changed every 45 days.

Three kinds of strategies have been described for ensuring the use of strong passwords. The first, which assigns the user a preselected, system-generated password, tends to produce passwords that are easier to forget, not being user-selected (Canavan, 2001). The second allows the user to select the password but checks for the password strength during password selection. The third, which postpones the check of password strength until some later time, allows for a more thorough check of password strength, at a cost of delayed feedback (Anderson, 2001). The last two strategies should require the user to choose a new password if the user's password is discovered (Anderson).

Kevin Mitnick has suggested five guidelines for combating social engineering attacks (as cited in Rosenberg, 2004). Always verify the identity of the person requesting confidential information. Verify that the requester is authorized to have the information. Avoid participating in telephone surveys because social engineers can pose as suppliers needing information about their customers. Avoid opening and replying to phishing e-mails—doing so can open a door for hackers and malicious code. Finally, avoid posting confidential information in plain view.

Effective Information Security for Higher Education Institutions

Information security policies should be formulated in accordance with an organization's business needs and practices. Some policies must be more restrictive than others. Higher education institutions need to consider academic freedom when developing and implementing information security policies (Elliot et al, 1991). Where possible, policies should be permissive enough to support the full exercise of academic freedom.

Camp, DeBlouis, and the Educause Current Issues Committee (2007) recommend that colleges and universities observe the following eight guidelines for information security:

1. Maintain privacy and security policies that (a) cover more than what is required by law, (b) are enforced consistently throughout the institution, (c) are reviewed and analyzed regularly.
2. Maintain a security incident response plan.
3. Maintain a plan to keep up with changes in threats and federal and state laws.
4. Make security a funding priority.
5. Designate a dedicated team for dealing with IT security.
6. Do a comprehensive risk assessment regularly.
7. Maintain IT security awareness and training program.
8. Maintain the appropriate infrastructure to implement protective measures.

Cate (2006) suggests that colleges and universities first commit to protecting private information, then reconsider the reasons for collecting the information they collect and the implications of collecting that information. This process should entail an assessment of the information collected and the reasons for collecting it, the risks associated with collecting it, and security measures that will be implemented to protect it. It should also provide people served by the institutions an opportunity to provide consent to collect the information.

Summary

The literature on information security indicates that information security issues continue

to challenge organizations including institutions of higher education. Studies report that authorized users played a critical role in protecting information resources. Several studies suggest best practices that institutions of higher education should follow for minimizing the risk of attacks on their information resources.

CHAPTER 3

METHODOLOGY

This study was designed to evaluate patterns of computer usage by faculty and staff members that could either protect or expose them or others to information security attacks. The study's participants were from ETSU, a regional state university, and Milligan College, a private college in Northeast Tennessee. ETSU serves over 13, 000 undergraduate and graduate students ("ETSU enrollment surpasses", 2007). Milligan College serves about 900 undergraduate and graduate students (Milligan College 2007—2008 Catalog, 2007).

Research Design

This study assessed behaviors of faculty and staff members that strengthen or weaken information security and investigated the relationship between these behaviors and information security awareness. In accordance with ethical research standards, approvals were obtained from the Institutional Review Boards at ETSU and Milligan College prior to conducting the study.

A mixed-methods research approach was used in this study. Snyder (2006) identified three types of mixed-method design: exploratory design, explanatory design, and triangulation design. This study employed triangulation design, which provides a more comprehensive analysis of a problem and enhances the study's validity. Qualitative and quantitative data are collected and analyzed simultaneously. The results of one method can then be used to support or contrast the results of the other (Snyder).

The study was focused on computing behaviors that users engage in as they do work-related tasks on computer systems. The study explored users' awareness of and conformance to best practices for password management, document and electronic recourses disposal, data back-up management, defense against malware, and defense against phishing e-mail. The study also explored users' knowledge of FERPA, which specifically applies to institution of higher education. Additionally, the study explored user' attitudes towards awareness and practice of

information security.

Qualitative Methods

Data Collection Procedures

The main data collection tool for the study's qualitative portion was interviews. The interviews were conducted with IT personnel at ETSU and Milligan College in order to get their perceptions of how faculty and staff members use information technology. The interviews were voice recorded and transcribed. Member checks, a peer debriefer, and an external auditor were used to establish reliability and validity. Reliability refers to the extent to which a particular research technique consistently produces the same results, given repeated studies of the same concept (Babbie, 2000). Validity refers to the extent to which the findings of a study accurately reflect the reality of what is being explored (Babbie).

Purposeful sampling was used to identify participants. Purposeful sampling is when participants who will be most informative about the subject are selected (McMillan & Schumacher, 2006). Snowball sampling, which is a purposeful sampling strategy, was also used. Snowball sampling occurs when participants refer the researcher to other potential participants (McMillan & Schumacher). The participants were information technology professionals at both institutions. Once potential participants were identified, I e-mailed or met with each and invited them to participate in the study. I explained the study's purpose and the participants' rights, then obtained their informed consent. The guide in Appendix A was used to conduct the interviews.

Additional, qualitative data were collected using question 40 on the survey instrument in Appendix B to evaluate faculty and staff members' attitudes toward the role they played in securing computer systems. The other 39 questions were used to collect data for the study's quantitative portion.

Research Question and Data Analysis

The constant comparison method of data analysis (Glaser and Strauss, 1967) was used to

analyze the qualitative data collected from the interviews to answer research question 1. The qualitative data collected from question 40 on the survey to answer research question 2. These research questions were as follows:

1. What are the computing behaviors of faculty and staff members that can either protect or expose them or others to information security attacks as observed by information technology professionals?
2. What are the faculty and staff members' attitudes toward the role they play in securing computer systems as reported by the faculty and staff members?

This method involves comparing one set of data to another and organizing the data into categories until a theory emerges (Merriam, 1998). An external auditor and a peer debriefer were used to assess the consistency of the findings with the information gathered from the interviews and question 40 on the survey instrument. The auditor and the debriefer also ensured that the information gathered was used appropriately.

Quantitative Methods

Data Collection Procedures

The online survey instrument given in Appendix B was used to collect self-reported data from the faculty and staff members at both institutions. Surveys are suitable for collecting self-reported data about the participants' beliefs or behaviors (Neuman, 1997). Surveys are usually used to collect data to test more than one hypothesis (Neuman). In addition, survey research is the appropriate method for this study because the study was designed to describe a population (Babbie, 2000).

This survey instrument, which was specific to this study, is a modified version of the Information Security Awareness (ISA) measurement instrument developed by Ryan (2006). The ISA measurement instrument consists of a user information security awareness scale, an information security practice scale, a personal innovativeness scale, and a computer self-efficacy scale. The survey's reliability and validity have been established through a face validity check, a

pretest, a pilot test (N=286—business students—72% return rate) and a factor analysis of the results from the full administration of the survey (N=531 out of 4,938 sampled) by Ryan. The alpha coefficients for each construct were above .80 (Ryan).

The survey for this study was adopted and modified information security awareness and information awareness practice scales. The survey had four sections. The first section consists of demographic questions that inquired about the participant's place of employment, gender, employment status, age, and the number of years of computer use. The next three sections were the user information security awareness scale, information security practice scale, and user attitude towards information security scale. The survey was self-administered online. The survey instrument is included in Appendix B.

Before using the modified survey to conduct this research, I conducted an instrument review with Educational Leadership and Policy Analysis doctoral fellows to test the instrument's validity and reliability. Alpha coefficients were computed to test the internal consistency of the awareness, practice, and attitude measures. The alpha coefficients for the awareness measure (.87) and the practice measure (.69) were acceptable. The alpha coefficient for the attitude measure was unacceptable (.18). Due to time constraints, a more reliable attitude measure was not constructed. Nevertheless, the questions for the attitude measure were included in the survey instrument. The data collected from these questions were used in the study's descriptive portion as well as in the analysis of research question 4. However, results related to the attitude measure in question 4 should not be considered reliable.

Population

The target population of this study was ETSU and Milligan College faculty and staff members including adjunct faculty and part-time employees. At the time of this survey, ETSU had an estimated 2,178 fulltime employees (ETSU Fact Book, 2007). Milligan College had about 230 employees, including fulltime faculty, adjunct faculty, and staff (Milligan College 2007—2008 catalog, 2007). Every employee at both institutions who had an institution-enabled

e-mail account was invited to participate in the study. At ETSU, permission to distribute the survey through e-mail was sought and received from the Vice President of Finance and Administration. The survey was then distributed through e-mail to faculty and staff members by the Associate Vice President of Information Technology. At Milligan College, the survey information was sent to the Vice President of Academic Affairs, who in turn distributed it to faculty and staff members through e-mail.

Research Questions, Hypotheses, and Data Analysis

Descriptive and inferential statistics were used to analyze the quantitative data. Statistical Package for Social Sciences (SPSS 15.0) was used to conduct the data analyses. The research questions, hypotheses, and data analysis methods are discussed below.

3. What are the faculty and staff members' computing behaviors that either protect or expose them or others to information security attacks as reported by the faculty and staff members?

Descriptive statistics were used to evaluate research question 3. They described the faculty and staff members' computing behaviors that either protect or expose them or members of their institutions to information security attacks.

4. In what ways, if any, do attitudes towards information security, awareness of information security issues, and awareness of information security policies make a difference in how faculty and staff members use information technology?

    $H_0$4: There is no relationship between information security attitude score, information security awareness score, and information security practice score.

Hypothesis $H_0$4 was tested using a paired-samples *t*-test to determine whether there is a relationship between attitudes towards information security, information security awareness, and information security practice.

5. What differences, if any, exist in information security awareness and practice among faculty and staff members with different demographic characteristics?

$H_0 5_1$: There is no difference in information security awareness scores between faculty and staff members at ETSU and faculty and staff members at Milligan College.

$H_0 5_2$: There is no difference in information security practice scores between faculty and staff members at ETSU and faculty and staff members at Milligan College.

Hypotheses $H_0 5_1$ and $H_0 5_2$ were evaluated using two-way analysis of variance (ANOVA) to evaluate the differences in information awareness and practice means between faculty and staff members at ETSU and faculty and staff members at Milligan College.

$H_0 5_3$: There is no difference in information security awareness scores among those who are 20—29 years old, 30—39 years old, 40—49 years old, 50—59 years old, and over 60 years old.

$H_0 5_4$: There is no difference in information security practice scores among those who are 20—29 years old, 30—39 years old, 40—49 years old, 50—59 years old, and over 60 years old.

$H_0 5_5$: There is no difference in information security awareness scores among those who had 15 years or less, 16—20 years, and over 20 years of computer use.

$H_0 5_6$: There is no difference in information security practice scores among those who had 15 years or less, 16—20 years, and over 20 years of computer use.

Hypotheses $H_0 5_3$, $H_0 5_4$, $H_0 5_5$, and $H_0 5_6$ were tested using one-way ANOVAs to evaluate the differences in information awareness and practice means among age groups and years of computer use groups.

$H_0 5_7$: There is no difference in awareness and practice scores among those who spent a daily average of 2 hours or less, 3—4 hours, 5—6 hours, and 7 or more hours on the computer (not on the Internet).

$H_0 5_8$: There is no difference in awareness and practice scores among those who spent a daily average of less than 1 hour, 1—2 hours, and 3 or more hours on the Internet.

Hypotheses $H_0 5_7$ and $H_0 5_8$ were tested using one-way MANOVAs to evaluate the differences in information awareness and practice means among daily average hours of computer use groups and daily average hours of Internet use groups.

Summary

Chapter 3 discussed the mixed methodology approach that was used to address the research questions. Selection criteria of participants, data collection procedures, and data analysis for each methodology were presented along with the hypotheses for the quantitative research questions were discussed.

CHAPTER 4

DATA ANALYSIS

The purpose of this study was to explore faculty and staff members' computing behaviors that either protect or expose them to information security attacks. The study used mixed-methods of data collection and analysis. Interviews were conducted with institutional technology (IT) professionals at ETSU and Milligan College and an online survey was completed by faculty and staff members at both institutions. The qualitative data and the quantitative data were presented and analyzed separately.

Perceived Faculty and Staff Members' Computing Behaviors

IT professionals at ETSU and Milligan College were interviewed to assess their perceptions of faculty and staff members' computing behaviors that either protect or expose them to information security attacks. Snowball sampling was used to identify participants. First, I contacted the assistant vice president of IT at ETSU and the IT manager at Milligan to get permission to interview people in their area. They referred me to potential participants. In total, I invited 10 IT professionals to participate through e-mail. Four from ETSU and two from Milligan College agreed to be interviewed. I used pseudonyms to protect the participants' confidentiality. The years worked in IT at their respective institutions ranged from 5 years to 18 years. Table 1 shows the participants' pseudonyms and the institutions where they worked.

Table 1

Participants and Their Institutions

Pseudonym	Institution
Allen	Milligan College
Ben	ETSU
Calvin	Milligan College
Fred	ETSU
Jim	ETSU
Ray	ETSU

The data from the interviews were analyzed to answer the following research question:

> What are the computing behaviors of faculty and staff members that either protect or expose them or others to information security attacks as observed by information technology professionals?

Password Management

IT professionals at Milligan and ETSU said that users' password mismanagement was the major challenge they faced. Four major issues with passwords emerged. Interviewees stated that users tended to use simple passwords, share passwords, write passwords on sticky notes, and, in some cases, to end their sessions without logging off. Allen summed it up this way:

> The password management, they [faculty and staff members] are very poor at it. They share their passwords with students. They share their passwords with other users. They leave their machines logged on and unattended. Basically, they have no respect for security, as far as the data on the network.

ETSU conducted a password analysis and found that users tended to chose simple passwords that could be easily guessed. According to Jim, ETSU has the evidence that users were choosing simple passwords:

> We [ran] an analysis on our passwords here on campus and have found them to be lacking in effectiveness…. So we do have absolute proof that passwords are not very secure. They are not complex. They are easily guessed by dictionary lookup and so we are taking steps to prevent that right now.

This was supported by Ray who simply said, "They do not use complex passwords."

Milligan College also faces the same challenge, as explained by Allen:

> No, they [Milligan faculty and staff] do not use strong passwords and we don't have anything other than the number of characters, as far as restriction on the password. They can use anything they want. Lots of times they simply use part of their name, you know, and basically they chose this because they share with anybody and everybody.

Another problem was password sharing. It appears that it was common practice on both campuses for users to share passwords with their colleagues and student workers. Calvin from Milligan said:

> I notice one of the problems we run into every now and then, because these things come up, we know that the faculty share their passwords with the students workers and other colleagues and things like that and we tell them not to do that but it always happens. I know that's a major problem because they, you know, will have a student worker call up and say, "I can't get logged in to so and so's computer. They gave me their password but it's not working." We will call them up and say, "You are not supposed to be giving student workers your password. It's not a good idea." But we, I mean, we try to tell them not to do that but I don't know if it's convenient or they just forget about it or think this isn't important. It's okay. They go ahead and do that. So, I know it's a major problem.

Ray from ETSU shared the same sentiment about ETSU users. He pointed out that in addition to sharing passwords, some users wrote them down and left them in plain sight where anyone can see them:

> Probably the number one violation of our Code of Ethics: they don't keep their passwords secure… They will give it to their graduate student, their boss, their co-worker. If that password is out, anybody, you know, that gets on that system- it's gonna look like it's the person. They do not safeguard their passwords. They write them on post-it notes [and] stick them on the monitor, stick them under the keyboard, you know, tell somebody. And I don't do that. That's my password. Nobody else gets it. The people down the hall they can change it on me but they can't look it up. That's some of the—that's one of the largest risk that we have. Example: yesterday we went to change out a computer in this project and the lady—her account was logged in but she's been on sick leave for several weeks. So somebody there has their password. And we see that kind of stuff a lot.

Ray also said there are exceptions—people who take the responsibility of guarding their passwords seriously. He said, "And opposite that, some of the behaviors we see are people that

guard their password so well they wouldn't tell it to me… there are other people that do safeguard their passwords well." This was consistent with what Ben said:

> In the password, the password management area, people tend to expose themselves by—well, it used to be that people would, would be very open sharing their password with other people. I think that over the course of the last several years, with all the exposures that, Internet scams and of all that, that people have tended to listen when we've told them, "Don't share your password." But unfortunately we have seen some instances on campus where a professor might share his password with a graduate student.

Instead of sharing passwords with graduate assistants, Ben said ETSU provides departmental accounts for use by graduate students. He explained:

> If it's going in to enter some information into something we have a technique called a departmental account that you know just some, some name that maybe related, like graduate school might have a gstemp account, Grad School temporary account, and then there is a password associated with that the graduate student gets and then uses that account to do the administrative stuff. And then on a periodic basis those passwords are forced to change.

The other problem that emerged was that a few users did not log off computer systems when they left the system. When asked whether faculty consistently logged off computers in the multimedia classrooms, Fred said:

> A lot of times when you wake up the computer, you will see somebody logged in. As far as security goes there, I mean, any activity you do will show up under that person, unfortunately…. That does happen. I see that, I don't know, maybe say if I look at a computer, maybe 10 computers a week, just I don't know how many but I would say at least 3 or 4 will have somebody logged in still.

While discussing Milligan faculty and staff members' password management, Allen said, "They leave their machines logged on and unattended." Figure 1 illustrates the password mismanagement problem.

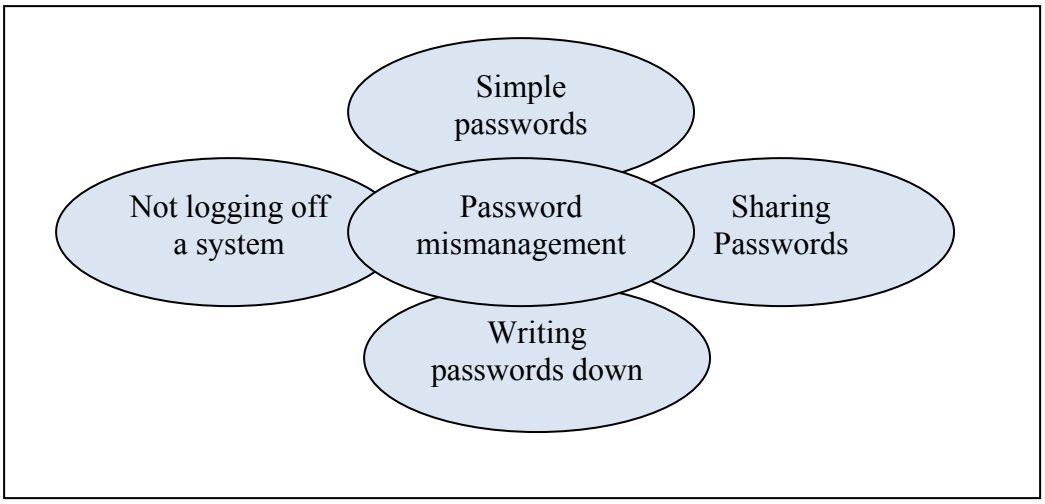

Figure 1. Password Mismanagement

Some participants gave reasons why users mismanaged their passwords. Ray attributed password mismanagement to attitudes not lack of knowledge. He said, "I think it's the attitude of seriousness. Some people do not believe how serious a problem it can be for someone to come and get into their computer and look around." Allen said, "Basically they have no respect for security, as far as the data on the network."

Ben identified password complexity as a reason for writing down passwords:

> Another thing is that you know, people tend to write down these passwords, if they are particularly complicated. If the password is complicated and they may not have used a technique for creating it that they can remember it easily, they write it down on a little piece of paper and stick it on their computer, something like that.

Participants also discussed actual or planned technical strategies for correcting the password mismanagement problem. Jim, from ETSU, said:

> We are in the middle of a process, right now as we speak, [of] activating Microsoft's complex password algorithms as a part of Active Directory. Active Directory is becoming our single repository for passwords. That's not—we are not there yet. We do now have single sign on and in moving in that direction it is apparent that Active Directory will become the repository of all passwords. We [have] a security committee that has advised IT and the IT Governance Council, the ITGC, and proposed and passed a policy for complex passwords. [The system] will retain previous passwords—I think it's 10 passwords that it remembers, the previous 10 that you cannot, you know, you cannot

> use any of those previous 10. You can only change your password once a day. So it's gonna be a long, drawn out process and hopefully most people get the idea, 'Okay, I understand I need to come up with a new password that's secure that I can remember.

ETSU did indeed implement this complex password policy on February 27, 2008, not long after this interview with Jim ("Campus-wide Password Policy," 2008).

Milligan College also forces users to change passwords periodically, although it does not have a complex password policy. Calvin stated:

> We don't force strong passwords although we have a minimum. I think a minimum of like 7 characters. We don't let them go below seven. I think—I will double check that but I think it's five or seven characters. We try to lengthen it a little bit so that they don't have a two-letter password or something that's really easy. But we do not force encryption as far as requiring them to do upper and lowercase letters and symbols and things like that. So we didn't wanna make it too difficult for them…. For password management I can tell you we implement here a forced change of password every—once a year. Some people do it more often. We force it once a year and we retain I think either 5 or 7, I think 7 old passwords. They can't reuse them.

This was supported by Allen who said, "Yeah, we, we force it twice a year. It's random. We don't hit the switch and say change passwords. I mean the computer just generally, just randomly selects and it's changed twice a year."

When asked whether the password mismanagement problem, specifically password sharing, would ever end, Allen said:

> I think there will always be passwords and I think there will always be management problems with passwords. When I see it becoming—getting corrected is when somebody falls victim to sharing their password. And something happens that—happens to them that they are accountable for because it was done on their login. They can't say it wasn't and they have no defense it wasn't them. Then that's when they learn—that's when they learn how important it is.

Portable Storage Devices and Laptop Security

Participants commented on the challenge of securing laptops and portable storage devices. When asked whether users were aware of the need to secure USB flash drives, Ray, from ETSU, said, "They are not. They are not." Allen from Milligan said, "Data storage devices, they leave them lying around everywhere. Anybody can grab it you know. As far as, you know,

JumpDrives, flash disks, anything like that, you can find them lying around everywhere."

Ray gave a specific example of an incident that occurred at ETSU that demonstrates the risks of portable devices in the hands of users who are not prepared to secure the data on those devices:

> And, also Judith, we have had people have laptops stolen. And you probably read of stories where, I think it was last year, a Veterans Affairs employee had one stolen that had lots of personal information. Laptops are not for that and they, they store confidential information on them and it's very much easier for someone to gain access to that data on the laptop. We had a nurse that had before and after pictures of surgical patients on her laptop. And she took it down to Best Buy. It's an ETSU piece of property. She took it to a Best Buy to have iTunes put on it so she can listen to her music. Essentially she turned it over with photographs of these individuals. It could have been a hand surgery, you know, it could have been breast enhancement but that young man at the counter had all of it. You can't do that. It's very hard to convince people that this is a serious issue.

As far as portable storage devices and confidential documents being left in multimedia classrooms at ETSU, Fred said, "People will leave stuff. Yeah, they do that sometimes. I don't see that a whole lot fortunately. JumpDrives, people are pretty good [at not leaving them behind]."

Participants admitted that the security of portable devices has not been fully resolved yet. Portable devices have recently become mainstream and the IT world is still exploring ways to secure them. One solution is data encryption, but it is not currently practical for many users. The most practical solution so far has been to raise user awareness and to discourage users from storing confidential information on portable devices. Ben said:

> Yeah, the JumpDrive, the prevalence of JumpDrives is a really sticky issue and it's not really something that, I think, we have fully come to grips with. The stories about information being lost through various government agencies losing laptops and losing JumpDrives that have social security numbers, we try to play that up as much as we can on campus, making sure people know about what happened, know why it happened, know why they should not do the same thing that that person who was at another institution did. It is a problem and there really isn't much of a satisfactory solution to it unless you actually go so far as to encrypt the, the data that's on the laptop and on the JumpDrive. And so many people don't do that because right now a lot of the computers [they are] going back to, say at home, may not be powerful enough to decrypt the data in a timely way so that they—they have performance issues in that. But just making sure people know about what other people have done.

While commenting on managing portable data storage devices, Jim pointed out that ETSU is currently developing specific policies regarding the protection of portable storage devices and laptops:

> As far as IT policies, there are none, currently, for disposal of JumpDrives. You see them [JumpDrives], they are everywhere. We have just alluded to a security committee, we have instituted a security committee and that is one thing that the new chair has been charged with, is looking at, at those kinds of policies. A sister university, Tennessee Tech, was recently exposed when a JumpDrive was lost and it had confidential information about students on it—no one wants that to be repeated here, so we will be pursuing appropriate polices there. We do, in our Acceptable Use Policy, talk about confidential data in broad terms but we don't address, you know, a specific type of a device.

Jim also supported data encryption as a solution. He noted that ETSU might implement that in the future, for laptops as well as desktops:

> One nice thing that we are looking forward to Vista for, it's a list of about one, is the ability to encrypt the entire contents a hard drive or a laptop. And we again have been talking about as Vista is implemented here that, that will be a requirement for any laptop running Vista and maybe even desktops because those can be stolen, those can be compromised but especially laptops.

Ray shared some practical advice regarding storing confidential information on USB flash drives:

> It is a very convenient method, but just like a laptop, confidential data should not go on those drives. They are too portable. They are too easy to lose. They are too easy to have them stolen. That type of data should be stored up on the network with the only way it can be gotten into is by logging into that user's account and if they don't give out the password, it will be secure.

Milligan encourages users to use the network storage space to store confidential information; however, Allen pointed out that security of the data on the network can be compromised by password sharing. He stated, "We do offer network storage space on our servers and if they've shared their passwords then whoever has their password has access to that."

Ray also expressed concern about confidential documents being left in plain sight where they can be seen by anybody who walks in. He stated:

> But I have been in offices, personally, where confidential information was sitting right above of the keyboard while the person was gone, you know, gone home for the day or

> whatever. They leave that stuff out. It's not just electronic confidentiality that's breached. They do leave their hardcopies of, you know, social security numbers, just about anything you can think about, you can find on somebody's desk any time of the day.

Disposal of Confidential Information

I could not identify any campus-wide document disposal policies at either campus. However, several offices have shredders and some offices at ETSU use a document shredding company to dispose of confidential documents. Ray said:

> It's becoming better. A lot of areas we have a contract with the document shredding company. And a lot of buildings or offices have the padlock bin. They put the paper documents in and they shred it at the truck and nobody else has access to it.

Calvin had this to say about documents disposal policies at Milligan:

> I know we don't have any policy that we tell them about, at least as far as, destroying documents. I know offices individually, Registrar's Office, our office and all that have shredders so that if we have confidential documents we shred them but as far as the individual faculty and staff in other departments—we don't at least have an overall policy. I don't know if one of the other offices have it or not. I haven't heard about it.

When asked whether users use those shredders, Calvin said, "I know, I know other offices do but, you know, I doubt the average faculty member [is] going have a shredder, so they may not be. They may be just dumping their documents in the trash."

Data Back-Up Management

The ETSU participants said that users usually do not back up their data. They had experienced cases where users lost their data as a result of a corrupted hard drive or accidental data deletion. Jim said, "It happens rather frequently, unfortunately. Most commonly is a hard drive that's going bad and they do not have a backup—a thumb drive copy or a USB drive copy of it in some way. Another is an accidental deletion." He added:

> We have invested in tools that will attempt to recover those files—deleted files or recover sectors of a disk that's going bad and those can take an inordinate amount of time so we do pay for that through, not only for the software, but we pay for it with time.

Ray said:

> Every day we get a call from somebody, "My hard drive died. Can you get my stuff back?" Sometimes we can, sometimes we can't. It just depends on the physical failure of the component. They do not do regular backups…. They don't do it. They don't take the time or they don't believe it's possible that they can be wiped out.

Then he added:

> It's a very hard lesson to learn but sometimes when it happens, they will realize the benefit of backups and they will start doing it…. You know, they are very diligent about it after they have had a catastrophe once.

Participants discussed how they dealt with those situations. They stated that each user and every department has allocated storage space on campus servers. The servers are backed-up frequently such that if the servers ever fail, the data can be restored. They encourage users to use that space to store their documents. Ben said:

> We have procedures so that all data on the systems that we managed are backed up once a week, what we call our full backup, and then after that we do what are known as differential backups where files that have changed since the full backup are backed-up every other day. So users on their desktops are generally covered if they have their data on the Q: drive…since that is on the common storage, that is on the server, that data is backed up on a regularly scheduled basis and information can be restored, if something is lost. But if the information is just on a local desktop, on a PC, then it is not stored by OIT on a regular basis, so the user, if they are interested and need to store that, then we tell them that they do their own backups.

Ray supported this and also added that users can use external hard-drives or CD to back-up their data.

> Those external hard drives, that silver box sitting down there, that's perfect [for] backups but they don't want to deal with it. Every new computer for the last 4 years has had at least a CD burner in it. They can burn a CD. Now if they are saving those data up on the network, on the server, we've got backups. We do it every night.

Jim also confirmed the use of server side storage. He said, "There is no required backup of desktop computers. We have encouraged departments to look at server side storage. We provide each department with a share, a drive share on one of the servers here." But he also described problems related to the misuse of server storage space:

> That becomes a double edged sword because then you will have a department that says, "Well, I'm going to save everything on the server" and they start putting personal pictures, music files, their iTunes library, things that aren't work related. So then that becomes a policing policy with disk quotas, with—and when it's a departmental share

> one person can fill all that up and then the department suffers because they can't store anything else that maybe important, may be work related because this individual has put their movies from their vacation up on the server. Policing that becomes a real problem, the overhead.

Allen, from Milligan College, agreed that users do not back up their data often on their own. Allen said, "That's, that's very common, you know. If any data backup is done, we do it for them. They have no concept of data backup. No they don't." This was supported by Calvin who said that data loss was infrequent because Milligan encourages users to store data on its servers:

> Fairly rarely. Like I said we try to encourage them to store their, at least, important documents up on the network storage as well so we can back that up and recover it for them. We have had some cases where if a hard drive had gone completely south and they have had everything stored there on the local drive that we won't be able to recover it for them. That's pretty rare, though. Usually we would run into a case, if someone's computer crashes and their hard drive is going bad we can usually recover the rest of their data off that drive. So that has been rare. It caused us some headaches obviously, if they haven't backed up their data themselves, extra work here. I can't really recall any case, well, not frequent cases were they have lost their data. Now we've had cases where, very rarely, maybe one or two since I've been here, where people have even stored something on the network drive and then immediately deleted it before we had a backup of it so therefore, we couldn't recover it for them because we didn't have a backup of it.

Defense Against Malware and Spyware

A few years ago, ETSU and Milligan struggled with malware risk management. Ray from ETSU said, "At one point 4 or 3 years ago we will get spyware tickets all the time." Jim supported this by stating:

> So in the past we have had people who have had hundreds of malware applications on a single computer at one time because one will download, another will download 10, others will download 50 others, and all of a sudden the computer becomes unusable.

Allen from Milligan said, "Two years ago, 3 years ago, this department probably spent 90% of the time cleaning spyware off of machines. Because we support the student body as well as faculty and staff, we spent 90% of the time doing that."

Ben discussed a specific incident where a user's actions caused an infection on the ETSU campus:

> Since I've been here we have had one incident where we were bitten by this. It was a user who had gone, I guess it was overseas, maybe Europe and when they came back, they brought their laptop over to the campus network and plugged it in and they had a prototype, prototype malware. It wasn't in production, shall we say, it had not been launched into the wild. Somehow they had picked up this prototype and when they brought it on to campus, it got on to our network and it took us 4 days to get things under control.

Participants said that user awareness of malware and how it infects computers has increased. Allen from Milligan said, "I think they are aware of it..." Calvin agreed and commented on the efforts they made to educate the users:

> I think they are….And I think we have done a fairly good job of, whatever meetings we have had and e-mails going out, warning people about what to expect and what type of things to look out for that could be adware and spyware.

However, Calvin said other strategies for managing malware made it difficult to judge the extent to which awareness translated into practice of safe computing behaviors:

> So, I think they are a lot more aware of that especially considering the fact that that would also, since they are getting blocked if they do click on something and they suddenly see it was blocked from our spyware firewall I think they will get the idea very quickly, "I shouldn't be going to sites like that, anything like that." So I think they are aware of it. A lot of it we do it for them, is the thing, and we try to keep any spyware software on the systems themselves including using the spyware firewall. So I can't say how much is knowledge we've imparted to them or they've gotten just in all been protected from that by the firewall.

ETSU's IT department, like Milligan's IT department, has made efforts to educate users about malware so that that user awareness of malware could increase. Ray said:

> Our users are becoming much more cautious and educated. We see that through our help desk records. We see trends over the years. At one point 4 or 3 years ago, we would get spyware tickets all the time and what we do is we go to the user and we explain what happened to them and we say well, you shouldn't go to this website, you shouldn't be doing this during work hours, it's not work related, that's how your machine got messed up. Some malware is so bad that we cannot fix the machine. We have to wipe it and rebuild. I mean, it's very insidious. But I do believe that our users, thanks to the people on the frontlines that go out and visit face-to-face and fix the problem, they will talk to them and explained to them how it happened and it changes their behavior. It does.

Ben also said users were more aware of malware, but he cautioned that the problem was still unresolved. Our conversation was as follows:

> Ben:

> Yeah, I think so. Although we have had some battles we have had to fight and I don't think we've totally won these battles along the way, but . . .
>
> Judith:
>
> What battles?
>
> Ben:
>
> There were some, there were some instructors that like to go out on the Internet and like to look for tools that they can use in instruction and you know, can't really fault them for that but unfortunately sometimes when they do that they bring things back in these, in these programs. So then they would have, you know have possible hooks in the program that could—so that the program can be used to download viruses or whatever, so we've tried to get, we've tried to raise awareness, I guess. Actually, we've tried to stop them. But we at least try to raise awareness that when they go download this free instructional package that looks wonderful there may be a price to pay down the road for all of us.

Ben's comment reflected one of the reasons why ETSU and Milligan College had struggled with malware during those years. Faculty and staff members at ETSU and Milligan College have administrative privileges on their office computers; this means that they can download and install any software. Jim explained the problem this way:

> But users are still administrators of their desktop and laptop computers. And right now any user on campus, any faculty or staff member can go out and format the C: drive and lose all their data or they can download a piece of malware and install it and we are not able to prevent that.

Ray elaborated:

> There are certain, there are some applications out there that will install whether you are an administrator or not but a lot of them if you don't have administrative rights, you are not gonna mess up the machine. Look at student labs. They are locked down. No student is an administrator when they sit down on the lab machines. It's extremely rare that the lab machine will be messed up with malware or spyware.

Although user awareness has increased, interviewees attributed most of their success in controlling malware to technical defenses that both ETSU and Milligan had implemented, rather than to changes in user behavior. Even though Allen acknowledged that users were more aware, he thought they depended more on IT to protect them. Allen attributed Milligan's success to implementing the Barracuda Firewall: "I think they are aware of [malware] but they don't care….IT can take care of it. IT can fix up that—what we mess up, you know. Barracuda has

really been a lifesaver." This was supported by Calvin, who said:

> And a large help though I think is the fact that we actually have an anti-spyware firewall that sits between us and the Internet and that's made a tremendous difference because even if someone tries to download spyware it won't let them. And if they, if they come in with a machine that's infected with it, the firewall will detect that and usually warn them they need to clean that up and offer them a little thing to clean it up with.

Allen also described, in percentage terms, how Barracuda helped them. He said:

> Two years ago, 3 years ago, this department probably spent 90% of the time cleaning spyware off of machines. Because we support the student body as well as faculty and staff, we spent 90% of our time doing that. Since we put Barracuda in, we are probably spending less than 1%.

ETSU also did not depend entirely on the users. Jim said:

> We don't want to detect it that way when the user says the computer is acting funny. It's already, it's already done something to that computer. And it can be very difficult to clean, so we do have more proactive steps in place.

For that reason, ETSU implemented Symantec products. Jim explained:

> What we have done in the interim is invested in additional [anti-]malware software. It is part of our anti-virus agreement with Symantec. The enterprise anti-virus also includes malware detection and cleaning. It does very good at detection. It does very good at cleaning. Sometimes we still have to do some manual intervention to clean a computer of malware but most times we are notified. We have a central server that all desktops talk back to and when they detect a virus or malware or anything, that central server is notified and an alert is sent out at that point that 'oh we've got a virus outbreak and it's been cleaned or we've got a malware situation over here and it's being cleaned or maybe it's not been cleaned.' So by instituting that we have actually prevented a lot of malware from being installed. We have also detected where it can be installed.

Ben supported this and also discussed another product they are considering for implementation:

> There are—one of the technologies that we are contemplating is what's known as NAC, Network Access Control and with NAC when a machine comes on to the network it automatically goes to a particular quarantine area where the machine is scanned to make sure that it has antivirus software, that it does not have an active virus of any kind on it. If it does not meet certain criteria then until it's uh it comes to the standards that it will not be allowed to get on to the general campus network. This is something we are working towards but we don't currently have because it's a very expensive solution. But yes, that, that generally speaking I can't think of any other instances where we have had uh a wide spread problem really although occasionally people do get viruses and we haven't had an outbreak because the Symantec software that we are using is very good.

Defense Against Phishing E-mail

Participants agreed that phishing e-mails are a major problem. The main problem is that phishing e-mails look legitimate. Jim described the problem this way:

> I sent a mass e-mail out ah this week or last week because a phishing attempt got on to campus that was for a local bank. Those are really scary to me. It's one thing when it's Washington Mutual Bank. We don't have that—any branches of that bank around here.
>
> And we hope people have some common sense to say, "Well, I'm not gonna do that. I don't bank with them," and delete it. But when you see one come in that's from the Tennessee Credit Union, which we have had happen, or a local bank like Carter County Bank…"

Ray gave a specific example:

> Last year we had three people who had their savings accounts at the Credit Union up here wiped out because they looked at a mail that looked legitimate, clicked on the link, filled out all the information and somebody ah they went and withdrew the money from their savings account.

ETSU's and Milligan's IT departments use spam filtering products and education to combat phishing. Communication with users is helpful in raising awareness. Jim said:

> We do use Brightmail, which is a software product that sits on a server and all e-mail coming in to campus is examined by Brightmail for spam and phishing is really a type of spam. It's an unsolicited bulk e-mail…. And we are rejecting anywhere from 60 to 80 % of the mail that is attempting to campus every day. Spam is that much. Most of the phishing attempts are being caught there. Sometimes they do get through and like I said, as recently as last week, I think it was last week, I put an alert out and I sent a mass e-mail out to faculty and staff saying this one got through. This is a hoax don't click on it don't do anything. Just delete it. And so we do—we are as proactive as technically we can be. But then we do try to be in a reactive mode so when someone tells the help desk, "Hey, I got this. Is this legitimate" or "I got this, this is awfully suspicious" or "I got this and this worries me" we do try to take action. And then we also—the other action we took, we not only send a mass e-mail and an alert, but we also went to the e-mail server. We said anything else coming from this address don't accept it, even if Brightmail has not been updated yet to, to delete this, to not deliver it, you don't pass it through to their inbox. So we do have controls at the entrance to campus for all e-mail and it's examined for spam, it's examined for viruses, it's examined for malware.

Ben supported this:

> Phishing really comes more under the spam fighting and uh recently we made some adjustments to our spam fighting so that now we are catching like 86% of the spam that comes into the university or—rather 86% of the e-mails that come into the university are being caught as spam and phishing is a small portion of that. We don't see a lot of

> phishing attempts that are marked as such by the software. But this is really more of an educational function here. If we see something that looks like it's a phishing attempt, then we try to get a notice out. If it's serious enough we put it—well, we get it out on a message to the, on the help desk phone line. Plus if it's serious enough we actually put it out on the ETSU alerts page on the website.

Ray said that users are also becoming more aware and proactive in verifying the legitimacy of these e-mails:

> They are becoming smarter and like a lot of times they will send me, they will forward it to me directly and say, "Is this a scam?" And I will respond, "Yes, point at the link and you will see it has nothing to do with that company." So they are, they are starting to think about it now.

Milligan implemented similar defenses. Calvin said:

> We have a spam firewall, not spam firewall, a spam filtering software that we run on our Exchange server and does a fairly good job of catching a good portion of the phishing. We block 80—around 80% of all incoming mail is blocked immediately as spam and that catches a lot of the phishing e-mails. Not all of them. We still get a leak—I get, you know, I don't know, maybe four or five a day still. We get a leak still. We have in various times especially when we have had a large influx of a certain type of e-mail come in we will send—if we have had a whole bunch come out, we send a blanket e-mail out saying this is a recent phishing scam that's come out. Please keep an eye out for it and beware not to do this. And we, every now and then, just remind faculty and staff, "Here is what to look for in a phishing e-mail." Even if it's not a specific example, you know. If it's asking you for personal information, if it's a bank you don't do banking with and things like that but not to click on it, or to call us, if they have any questions about it. And some of our faculty are also very good about it. If they get something that's warning about a virus or phishing or all that, they will send it to us and say, "Is this legitimate or not", which is good.

FERPA Awareness

The participants declined to make judgments about FERPA, on the grounds that their respective Registrar's Offices were responsible for assuring FERPA compliance. Allen said:

> As far as FERPA, that is really handled through our registrar's office. They do all the education on that and—with the faculty and staff and keep us up to data uh and keep us notified of consent and all that so—okay.

Jim said, "The FERPA compliance office is really the Registrar's Office, it's not IT." However, he also noted that users who have access to the student information systems at ETSU are presented with a FERPA statement every time they log in to the systems. Whether they read

it, Jim said, cannot be determined:

> We are in the process of migrating to a new student system. Today's system, every time a user signs on they are presented with a FERPA statement. They should be aware of it. Now many people get into the habit of typing SIS (for Student Information System), SIS enter, enter and it flashes the screen up and maybe it goes away. But it is displayed every time they log in with the current system. The new system, we have not put that in place yet but we are not in true production on that yet….

Ray said he thought that users were aware of FERPA but did not understand the implications of violating FERPA guidelines:

> We have had examples where a parent had accessed a student's grades by virtue of her job position. You know, she was supposed to help other students. She went and looked up her kid's grades…. She was an employee, her child was a student. She had no reason to look at her child's grades but by having access to the records, she did and she said something to the child and the child became extremely unhappy with ETSU because those were suppose to be private. That person, even though it was a parent, had no reason to be looking at her grades. So that was a large violation against FERPA guidelines. I don't know the outcome of that situation but those are the type of things that can happen. They are aware of it. I just don't think that the seriousness of it has—not sunk in, I don't believe.

Academic Freedom and Administrative Privileges

ETSU and Milligan College grant faculty and staff members administrative privileges for their office computers. ETSU's IT department would prefer to grant users administrative privileges on an as-needed basis but have not been permitted to implementing this policy because the faculty and staff have argued that removing these privileges impedes academic freedom. Jim shared his experience:

> We talked about this one when you came to visit earlier and the, the ability or the accessibility of free software on the Internet has been something we have really struggled with here. We have at times tried to restrict the privileges that individual users have on their desktop and we have not been successful. IT has presented a very strong case that there are vulnerabilities and the fact that all employees have administrative rights to the computer, their primary computer is a serious concern to us. The governance committee that we have, the structure that we have here never thought that the benefit outweigh the downside. So that has never been instituted…. But users are still administrators of their desktop and laptop computers. And right now any user on campus, any faculty or staff member can go out and format the C: drive and lose all their data or they can download a piece of malware and install it and we are, we are not able to prevent that. Oh, they can

download good things too. I mean, they can go get real educational tools or tools for research and that's the, that's the side that always gets heard louder than us about the security risks – is the, "Oh, I need that for my class." And their argument has always been, "Yes, computer science, they need that. Yes, technology may need that." But the secretary in the psychology department probably doesn't. The clerk in Bursar's office probably doesn't. And we have done some pilots, and this was fascinating to me, it didn't carry enough weight for anybody else, but we went into a particular department in the administration building and we made a deal with them. We said let us keep your people from being administrators. We promised we will address any needs that they have. Because they were coming, they had several employees that, that loved to go and surf the internet and download things and you know. It's a screen saver or it's a picture viewer, you know, something free is the hook. And they'd go in several days a month and the computer will be unusable because spyware, malware will be installed on it and they couldn't do their business. So we made a deal with them and said, you want to come in everyday and do your business, right? Let us do this. Let us remove administrative privilege and we will promise to do whatever it takes to keep your, your software loaded and up-to-date. We'll do that for you but we will also guarantee that your computer is going to work at 8:00 every morning. And they agreed and it did and it worked and they don't miss it. We tried to use that as proving grounds and hold that up to everybody else. We just have not been real successful with that.

Ray shared the same sentiments:

There are certain, there are some applications out there that will install whether you are an administrator or not but a lot of them if you don't have administrative rights, you are not gonna mess up the machine. Look at student labs. They are locked down. No student is an administrator when they sit down on the lab machines. It's extremely rare that the lab machine will be messed up with malware or spyware. But we attempted to not give everybody administrative rights some years ago and we were shut down with a loaded canon. There is no university policy that says who gets it, who doesn't. By default they told us everybody who has a computer at their desk can be an administrator. We do not allow students to be administrators on faculty and staff machines but when you give the faculty or staff administrative rights, they can sit down and make the student an administrator.

Milligan College IT professionals differed from ETSU IT professionals regarding administrative privileges. Allen said:

I'm fine with it [administrative privileges]. As far as our lab environment, we have those secured, you know, depending on your, your login, what you have access to. But as far as the local machine, we give them, we grant them full access to the local machine.

He also said:

Well, the thing about it is there are so many things that an individual may use that you can't say no you can't have it or yes you can. And if you got them secured you are

loosening that security all the time to let them do something or you are running over there to login as an administrator to do that for them.

Calvin agreed:

I usually prefer that people not have admin privileges on their local system but it hasn't become an issue as far as systems getting, you know, run out with spyware or viruses, and things like that. If that became a large issue we might have to revisit that but thus far it hasn't been a big issue, so it is the convenience that it offers them so that we don't have to go and install things for them and all that, and a convenience for us. The savings in time is worth a lot at the moment at least.

A statement by Ray summed up participants' perceptions of faculty and staff members computing behaviors that affect their exposure to information security attacks:

But I would say the two primary issues that ETSU deal with as far as the desktop, password management and giving everybody administrative rights. You know, that's the biggest problem for my group in particular, you know. But, you know, on the bright side the users are becoming more aware. They are becoming more educated about safe computing practices.

Ethics of Computing

Participants in this study repeatedly raised concerns about ethical and legal aspects of computer use, especially with respect to pornography, using university computing resources to run a personal business, and peer-to-peer file sharing. My conversation with Ray was as follows:

Ray:

Probably the only other thing that we at ETSU have issues with as far as security, there are legal aspects to computing and I don't know if human resources shares that with them in orientation or not but they are certain things you can't do. You can't look at child pornography. That's illegal. You can't. And then other things, Judith, I believe that are important that are not really shared with the employees are the ethics of computing. You shouldn't sit in here and run a home business from your office computer and they do.

Judith:

It actually happens?

Ray:

Yeah. Pyramid schemes—you've heard of pyramid schemes where people wrap in one person, who wraps in another. Nothing ever exchanges hands but you pay a fee to be a representative of this company. It's crazy. We had somebody who ran her pyramid

scheme from her ETSU computer. And sometimes we are just not given the power to do anything about it except to tell them no, you can't do that.

Jim also said:

> We have been involved in cases, legal cases, where employees have sent improper e-mails or employees have been doing inappropriate things at work with the network. We have invested in computer forensics software that will undelete deleted files, will look through slack space on, on clusters of sectors of the disk and with the size of the hard drive today getting so big and the ah cluster size getting to be such a large number sectors, it's very common to be able to find whole files that nothing shows it's there but this forensic software will go get it. And we've been asked to look for memos and spreadsheets and child pornography and regular pornography and doing commerce on campus, which is not allowed. I couldn't set up a private business, you know, and be selling things from my desktop computer here and we've had people doing things like that.

Participants from Milligan College and ETSU shared common concerns about peer-to-peer sharing. Jim commented on peer-to-peer file sharing:

> Another thing is peer-to-peer trafficking. Music, movies, software—everybody likes music, everybody would like their music to be free. Everybody enjoys watching movies. They would like for them to be free. And there are people who trade in those things on the Internet and we are held accountable for that. The University is held accountable for what employees and students do.

Allen shared the same concern:

> I have a real concern about the sharing of copyrighted material through networks and we take action against here at, you know, here we discourage every faculty. If we find it we stop it. You know we do have thing in—as a matter of fact Barracuda is our content filter. So we have content filter on the network. We also block peer-to-peer sharing of music and things like that.

ETSU and Milligan have established procedures for addressing ethical or legal problems that arise from inappropriate computer use. Jim stated that the Human Resources department usually gets involved. Jim said:

> So when we, several years ago, when we started seeing an increase in that kind of activity, we found ourselves as being kind of the judge, jury, and executioner and we didn't want to be that. It was—it was not wrong to OIT for someone to, while they are being paid, trafficking pornography. It's really a human resource issue, so we got that restructured. That's why you will see our acceptable use policy is now a human resources policy because it is your employment with the university that you are abusing as much as you are abusing our resources too and you are misrepresenting the university in bad light. So now when, when an incident is detected, if someone reports it to us, we just send it to

> HR then HR comes to us and says yeah, we have looked at this and I think we have got an issue here.

Users should understand that their computers and the data on the computer belong to the institution. Jim said:

> And it is the University's data, even if it's a personal e-mail from a family member. That data belongs to the University. That's spelled out in the policy and that's what everyone agrees to. And I was telling you about that that they are apprised of it during orientation. When they sign on that's what they are agreeing to. Those have been the stickiest issues.

Allen expressed an opinion that users have responsibility to use information systems ethically:

> I think we've got to educate our students, our faculty and staff, you know, that it is wrong, ethically, you know wrong, morally wrong, you know, and try to keep that in front of them. I think they have to be held accountable for what they do. Just because it's there doesn't mean it's right. Yeah, that's, that's an individual's decision.

Jim noted that the university has limited authority as far as controlling what users can access on the Internet. The university, as an educational entity, cannot restrict user access as much as those in the private sector can. Jim explained:

> So we have put in—and we are a university and we are not about blocking or censoring information. We are not and we are very different from a corporate entity because of that. If we were Tennessee Eastman, you know, if it wasn't a chemical website, you know, we can say, that's not appropriate. We don't want you to be looking at the New York Times. We don't want you looking at it because it's not part of your job, your reason for being here. We are a university. We have all kinds of people studying all kinds of things. We have had people doing research projects in child pornography—in political science and criminal justice. And if those are approved, kind of like your project was approved, we wouldn't take any action. I mean, if they are helping solve these issues, why would we want to stand in the way of that—looking for abused and missing children. We wouldn't want to [impede] that. We have a College of Medicine. If someone wants to look at anatomy—some people may consider that pornography, but there are anatomy classes here. There are art classes where nude models are in the room with the students here. How do you block a picture of a naked human body and not infringe on their rights to be a student of that. So I do understand academic freedom and I do respect it. I just think there are limits to that excuse.

Milligan College, a private college, can restrict access to some kinds of information that ETSU does not control. Allen said:

> Here we have a lot of filtering on our network. Our—we filter content, we filter pornography, we can filter gambling, we filter—we block a lot of stuff, you know, and we get a lot of complains about things being blocked, but it happens.
>
> Allen added:
>
> See we are private, we are a Christian oriented school and when you come here, you know, you are expected to have these morals and you know, we try to protect those morals and instill those morals but I don't really know if we do real well by blocking it. You know, the temptation is not there, you know, in a lot of ways, so I don't know how well that's teaching anything.

User Awareness Programs

The IT departments at ETSU and Milligan College use several methods to communicate urgent and nonurgent information security messages to faculty and staff members. ETSU uses mass e-mailings, an alerts webpage, and a text messaging system to communicate urgent messages to the ETSU community. Jim said:

> We use several different notification methods. Most commonly we use ah mass e-mail. We also use the alert page on our website. We have recently instituted a text messaging system that could be used for things like that. Those are for kind of immediate outbreaks.
>
> Ray added:
>
> We here at ETSU, not personally but as a department, we use e-mail a lot, mass e-mail. If there is a new type of phishing e-mail coming out that looks legitimate we determine if it warrants an e-mail to go out to the campus community.
>
> Ben said they also used the help desk:
>
> We usually, what we, what we tend to do is to funnel this sort of information to our OIT help desk, both the faculty and staff help desk, and the student help desk, if there are any issues that we identify on the serve side.

According to Allen, Milligan College relies mostly on e-mail, "Usually the—our, our main means of communication is by e-mail, campus-wide. We periodically send out e-mail issues, you know, anything dealing with security: spyware, patches, things like that. All goes through the e-mail." Calvin supported this by saying, "Mainly [in] my job I e-mail. If we had a security issue that I think needs attention or their attention, I usually bring it to their attention by e-mail."

Training Programs

Figure 2 shows the types of user awareness and training programs offered to users by ETSU and Milligan College.

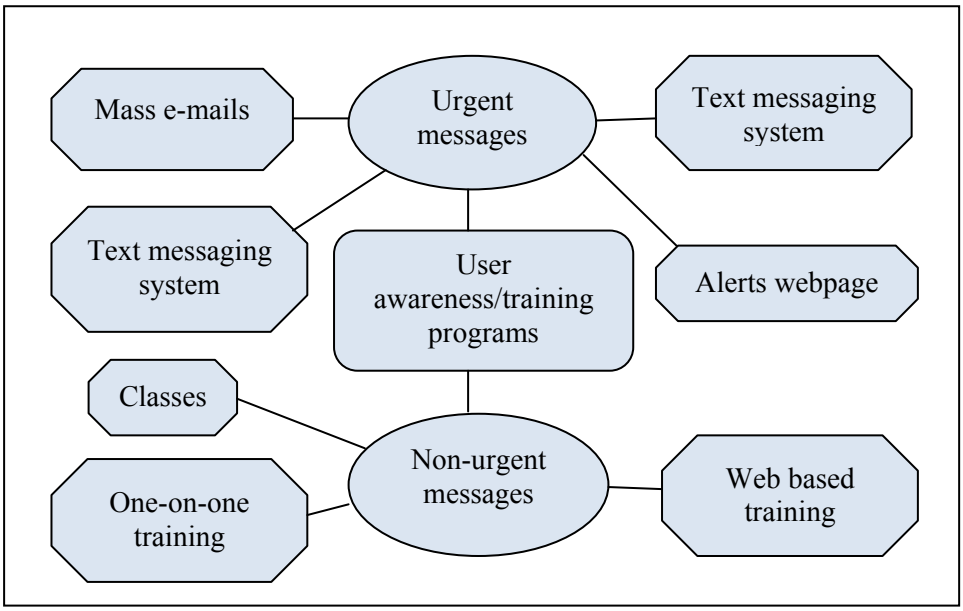

Figure 2. User Awareness and Training Programs

At ETSU, classes are offered through the Academic Technology Support office. Jim said, "Through Academic Technology Support, we have offered courses in security awareness, in protecting yourself from viruses, spyware, things of that nature." This was supported by Ben who said, "Usually most of the training related to technology is handled through the Academic Technology Support group" and by Ray who said, "Personally this group doesn't have a formal training. ATS/E-learning, formally they were part of OIT now they are under Academic Affairs, they have workshops that they schedule and offer." When asked whether there were any training programs for faculty who used the multimedia classrooms, Fred said, "The official policy is they go to ATS. They are trained and then they are certified. They get like a key to the equipment cabinet and stuff like that."

Another course taught in conjunction with the Human Resources Office was discussed by

Ray:

> I do a workshop for Human Resources twice a year. Well, it is titled: "Becoming Aware — Becoming IT Aware at ETSU". Ah unfortunately we have more existing employees coming than new people (more are current, long-term employee rather than new hires) but it covers a very wide range of— from obtaining to using computers at ETSU and we emphasize at that time safe computing practices. We share with them that information.

Jim also said, "We have a website also that is designed to serve as training to people about security issues." They also take advantage of one-on-one interactions with users to teach users safe computing behaviors, as expressed by Ray:

> And, as a group, we have people assigned to be responsible for certain areas on campus. They do a lot of one-on-one education. They will talk to the users. They will explain things in layman's terms and emphasize to them safe computing behaviors, is what we like to call them, how to practice safe computing.

Fred added:

> We do deal with users quite a bit. Used to be I was actually involved in training as well but now it's a lot of times if the faculty—most of the faculty problems we get are faculty not knowing how to use the systems. So we go there and try to show them how to use it. But they have problems with installing software and stuff, so we do have a lot of face to face contact with faculty.

Milligan College's IT department also offers information technology courses regularly. Some courses are taught by Milligan faculty members. Allen said:

> Now throughout the course of the year each semester we provide classes that are taught by other professors, our help desk manager teaches some classes, things like that, on applications that they use. Okay and this is done as a group, volunteer to sign up. You know, if you want to come you can, if you can't that's fine. We usually try to do those monthly but it ended up more like quarterly, trying to get it scheduled, but we talk about things, you know, we talk about Outlook, using Outlook, you know, archiving your e-mail, backing-up your machines. How to maintain your machines from spyware, malware, you know, things like that. So, you know, general things. Now we do do some departmental training too. That's specific to software a particular would use.

This was supported by Calvin:

> Our department as a whole has training programs every now and then we offer for faculty and staff on different security issues whether it's e-mail scams or phishing or keeping their computer protected from viruses or spyware. Getting them to come is another matter but we do offer them every now and then.

Computer use policies are also used to educate users. Allen said, "We do have a

Computer Use Policy that all of our users consent to go by—just when—they acknowledge it when using the network. When they log on they are granting consent." Jim, from ETSU, said, "They are made aware of the policy, the main Acceptable Use Policy that they are agreeing to by using their account and that in turn tells them about security and proper procedures and some things."

New Employee Training. In addition to its semiannual "Becoming IT Aware" workshop (see above), ETSU offers new employees minimal training in safe computing practices. Jim explained:

> New employees have to go through the new employees' orientation as part of the human resources—it is a requirement—and there is an IT component in there, where they are made aware of the resources available to them. There is nothing specifically about computer security there other than the fact they are made aware of the policy, the main Acceptable Use Policy that they are agreeing to by using their account and that in turn tells them about security and proper procedures and some things. Not a lot of depth but it does start them down the path towards being aware.

Milligan College offers no specific training for new employees but does offer courses throughout the year for anyone interested. Allen said:

> We don't really have anything scheduled as far as for new faculty or anything like that. Once we give them an e-mail login, network login, Angel login then they pretty much are on their own as far as that is concerned. Now throughout the course of the year each semester we provide classes that are taught by other professors, our help desk manager teaches some classes, things like that, on applications that they use.

Calvin supported this by saying, "There is not [new employee training]. We talked about that in the past but we do not have any specific training when someone new comes in to—that they go through"; but, he added, "It's a good idea."

Relaxed Attitude. ETSU's and Milligan's training and awareness programs available for computer users appear to be totally optional in that even mandatory attendance policies are not enforced. Fred noted:

> But yes, the official, the official policy is they go to ATS. They are trained and then they are certified. They get like a key to the equipment cabinet and stuff like that. But a lot of teachers fall through the cracks because we have classrooms all over campus so the teacher will teach there whether they have been trained or not. Sometimes they don't know they have to go through training

Ray noted a lack of interest on the part of ETSU's faculty and staff. He said, "They [ATS/E-learning] have workshops that they schedule and they offer—participation is not as high as we would like." Calvin indicated that the same was true at Milligan College. He said, "Our department as a whole has training programs, every now and then, we offer for faculty and staff on different security issues …. Getting them to come is another matter but we do offer them every now and then." Allen also said, "We usually try to do those monthly but it ended up more like quarterly, trying to get it scheduled."

Faculty and Staff Members' Role in Securing Information Systems

One open-ended question on the survey asked faculty and staff members to comment on the role they play in securing information systems. Of the Milligan and ETSU faculty and staff members, 449 responded to the survey and 166 of the 449 responded to the open-ended question. The responses were assessed to answer Research Question 2: What are the faculty and staff members' attitudes toward the role they play in securing computer systems as reported by the faculty and staff members? The responses provided an insight into what users state about their responsibilities and the challenges they face in securing information systems. Faculty and staff responses also revealed differences in awareness and practice levels among the participants.

Authorized User's Responsibility

Overall, most of respondents indicated that they had some responsibility in securing computer systems. One participant said, "A computer system is no more secure than its least secure user" (P110). Another said, "It is a responsibility and not an option" (P337). One respondent from Milligan said:

> Because we are such a small school, I believe we all have a duty to follow security measures to the best of our ability. Although I have never had formal training on our system, our IT dept. is always willing to answer questions and share updated information. (P32)

Another from ETSU said:

> I understand the importance of securing not only student information but institutional information as well. I know there are unethical people that would love to access our systems here at ETSU. I pledge to always protect the information that I have access to and all the files I create through my job tasks. (P153)

One participant commented on a lesson learned from a personal experience:

> I have learned much since my personal identity was stolen 2 years ago and take measures to ensure it never happens again. I heavily rely on my computer to do my job and safeguard it as much as I can. (P207)

Others discussed the role of users in general terms, emphasizing the vital role authorized users play in securing information systems. One said, "It's important to be consistent in protecting sensitive information. It only takes one [person] lax in security to compromise the entire system" (P165). Another expressed the same opinion, "The end user is one of the most important person in making sure passwords, systems security, etc. is continually updated and accessible to only that person" (P326).

Others said:

> In any situation involving security, humans offer the greatest potential failure point. This is true whether addressing physical security, security of classified information or computer security. It is no accident that individuals, who are proficient in penetrating security systems, concentrate their efforts on humans. In particular with regard to computer security, social engineering is the first method of choice. Only through periodic training (retraining) can this weakness be reduced. (P113)

> As staff I believe we are the first line of defense in keeping security practices at the University. We are very fortunate to have an IT person in our department who keeps us informed on these practices and reminds us of these frequently. (P146)

Another said:

> I feel I do my part in keeping my computer secured. I never leave my computer unattended to where someone could use it without my knowledge. My computer is usually locked when I am not using it. Also, I can lock my door when I leave so therefore I feel like it is more secure than if it were in an open room or cubicle. (P17)

Levels of Awareness and Computing Practices

Faculty and staff members' comments revealed differences in the level of awareness and comfort with technology among the participants. Four types of users emerged from the comments. The first group seemed to be technologically savvy. They seemed to be very aware of information security issues and diligently practiced safe computing behaviors. It appeared they could keep up with information security issues independently. They said the following:

> I typically back up files using at least three (3) different physical media (e.g., desktop HDD, USB drive (end of day), and back-up to a 2nd HDD (at 1:45 a.m.)). I also periodically make data back-up using CDs (740Mb) or DVDs (2Gbs) as "snapshots" in case of system or HDD failure. For personal and consulting work, I use E-mails that are digitally signed and sometimes encrypted. When traveling (especially overseas) I do not take USBs or laptops that include confidential &/or proprietary data; hotel systems are proven sites for predatory industrial espionage and snooping. (P383)

> I think I have an obligation to myself and my department to be vigilant concerning computer security. I also feel it is important to pass information on to everyone in my department concerning computer security to keep folks from being complacent or developing bad habits. (P242)

The second group, the largest of the four, included people who took their responsibility seriously but needed help with keeping up with information security issues and technologies. They said they thought they were responsible and they did their best to protect information. Some indicated that they wanted to behave responsibly but were not prepared or educated to make the right choices. One said, "It is my responsibility to be sure my system is secure. If I cannot do it, I must call on our computer professional to help me do it" (P437). Another said, "In my role, I am sure I am responsible. I probably could use some training on making sure I take care of information responsibly" (P195). Yet another said, "I try to follow the basic security precautions, but I am reliant on what other people tell me since I do not go and seek out information on my own" (P449). Others said:

> The role that I play in securing computer systems is to be aware of constant changes and be willing to learn. The role that the University plays is to deliver updates and information to employees to ensure awareness and compliance. (P196)

> I do what is necessary to make sure confidential information stored on my computer remains secure. I feel I am a responsible computer user. (P389)

> I take security seriously, but I try not to be paranoid. (P44)
>
> It is difficult to keep up with computer technology and protection. Because I am unsure about what the best practices are, I play it very safe ""at home"" and am very behind the times. At work, I rely on OIT to take care of the computers, so I follow the rules to the best of my knowledge. (P367)
>
> I try to do my best to keep my computer and files as safe and secure as possible, but nothing is 100 percent guaranteed safe.
>
> I do what I am asked to do. (P23)
>
> I follow the directives that come through ETSU, including purchase of security software for my home computer. (P53)
>
> I am confident that I handle confidential material in accordance with this institution's policies. I seldom log off or lock my computer during the work day because I lock my office door when I leave the office. In my work environment, this seems to be sufficient for security purposes. (P82)

The third group included people who used computer systems minimally or ignored the information security issue. One said, “I don't know anything about it, so I don't really worry about it until the problems on my computer are too big to ignore” (P18). Others said:

> I just do not use the computer instead of ""bothering"" people to find out if something is secure to do/perform or not to do/perform. I am too new to computers to fully utilize them to the full potential. Frequently I just turn the screen off on the moniter [*sic*] and leave the office for a short period of time. I have been told that the locking down of the computer is easily broken; so, I wonder what the use of even doing that is. (P309)
>
> It is sometimes difficult to remain current on the most up-to-date information. I sometimes get confused trying to understand all of the security issues, so I do not use the internet for banking. I have used it a few times to place orders, at Christmas time, over the internet, but prefer to call to place an order. I would like to do more financial transactions over the internet, but my lack of knowledge/confidence in computer systems makes me reluctant to use it. (P249)

The last group included people who did not act responsibly. This group included people who seemed aware of how their actions could expose them to information security attacks. One said, “I am not very helpful in securing computer systems” (P265). Another said, “I rarely consider the role I play in securing computer systems; however, I do realize how wrong I am” (P414). Some said they thought security was the responsibility of IT departments. One participant said, “I depend on OIT to keep my computer safe as I am not computer savvy” (359).

Some indicated that convenience was more important. The rest of the comments were as follows:

> To be honest, computer security is not a topic that I think about. I am aware of the issue and the challenges, but don't put my knowledge into practice when I use my computer. Unfortunately, too many times I view my computer like a file folder that I keep in my office. With my paper folder, I do not secure my folder in a locked file cabinet. In addition, I clearly label the file folder using a word that defines the content of the folder. My primary concern with my paper archives is immediate and easy access. I feel the same way about my computer! Access is of primary importance to me. (P333)

> While I am keenly aware of issues related to computer security, I must confess my knowledge does not always result in appropriate action. Too often I delay performing tasks such as updating protection and backing up files. (P37)

> I am not good at dealing with these things. I am admittedly too trusting. I don't feel I have time or energy to put into acting like I have to guard myself as if my identity and life could be stolen out from under me at any given moment. Perhaps I am foolish for feeling this way. I do only part of what I need to do for security, and that's mostly so a virus won't kill my computer most of the time. (P229)

It also appeared that some of these differences might be a result of users' job functions. Participants who worked with confidential information such as student records or patient records or those who worked in IT indicated a strong sense of responsibility compared to those who did not usually work with confidential information. The following comments reveal these differences. One participant said, "I don't work with security items" (P185). Another who worked with student records said, "I have to keep my computer secured due to the amount of confidential records we have on students in our office" (P160). Another said, "I work in the College of Pharmacy; that was not an option" (P189). Others said, "I manage a number of campus computers in classrooms. I am vitally aware that security is essential" (P73), and:

> Keeping up with computer security is an ongoing in my profession as well as my personal life. I am careful at ETSU to follow recommendations from OIT and use the internet solely for internet and library searches, and e-mail. At home, I face many challenges as the parent of two teenagers. I monitor their use of the computer, their selection of usernames (It as a shock to me that my then 9 year old daughter had the username of 2hot41guy at one point), discuss with them almost daily the threats and possible misuse of computers, and attempt to educate their download and use of on-line games, programs, etc. (P203)

> My career prior to coming to ETSU was as an IT security manager in an electronics firm. I am a Certified Information Systems Security Professional (CISSP). Information Security was and is my business. (P86)

One indicated that conditions at work sometimes caused him or her to engage in unsafe computing behaviors, stating, "I think I understand the concepts of security, but in our department we have to cover for each other from time to time. We are required to share password information and keep everything accessible to each other."

Role Models

Some took their responsibility a step further. They indicated that it was also important to be a role model for others. One stated, "I think educated faculty need to be role models for others and encourage good practices" (P29). Another said, "By following good security practices myself, perhaps I will be an inspiration to others to do the same" (P157). Others said:

> As a supervisor I must set the example for the people who work with delicate and private information. If I don't exhibit my awareness for complete compliance with the measures in place, then my staff won't see the need either. (P223)
>
> Individuals should play a large part in keeping the whole system secure. We all need to follow the policies that are in place to protect the system, but I don't think that many people actually know what the policies are. (P176)

Work Load

Some participants indicated that they simply have too many responsibilities to pay attention to safe computing practices. These users depended on the IT department to protect them. One said, "I try to keep up and help, but trying to get everything done sometimes results in forgetting to do the things that I should to keep information secure" (P215). Another said, "While I am keenly aware of issues related to computer security, I must confess my knowledge does not always result in appropriate action. Too often I delay performing tasks such as updating protection and backing up files" (P37). Others said:

> I do not have the time to invest in studying security issues in-depth and rely quite heavily on the technology services at the University for the security of my work related files / issues. I try to comply and hope I am remembering what I need to do to comply with the suggestions of OIT. It is hard to remember all that may be necessary. (P311)

> Our students rely on clean secure files, especially in D2L based CMS and the instructors should be careful what they share on these platforms....the electronic workloads are ""lost time"", unremunerated and probably > 20 hrs a week off the clock after classroom and administrative work...administration is complicit in poor security as faculty are so tired they can easily fail to manage every aspect of eSecurity of files and systems. (P315)

The Institution's Responsibilities

There were several comments about the institutions being responsible for educating users about information security issues and providing solutions. These comments came from ETSU participants. One user said, "Nearly all of my computer work is work-related. I rely on OIT for updates, ant-virus and other protections, and other information" (P66). Another said, "I do not have the time to invest in studying security issues indepth and rely quite heavily on the technology services at the University for the security of my work related files or issues" (P311). Another said:

> The role that I play in securing computer systems is to be aware of constant changes and be willing to learn. The role that the University plays is to deliver updates and information to employees to ensure awareness and compliance. (P196)

Some stated they thought that IT departments were very helpful in providing information and recourses. These said:

> ETSU OIT has been extremely helpful in teaching me how to backup and secure my work and computer. Having worked in other places without a strong IT department makes me appreciate them even more. It is my responsibility to be knowledgeable about protecting my computer and OIT helps me do it. (P80)

> I've never really thought about my role in securing computer systems, so I have no feelings about my role. I do have feelings about ETSU's role, and I believe the university has a responsibility to its users, which I believe it fulfills. (P96)

Others said they felt their institutions and IT department could do more. One said, "Computers are hardly mentioned in new employee orientation. I feel that I could improve in my role." (P173). Another said, "I believe we play an essential role and it would be very beneficial if ETSU could assist its employees with the education of maintaining reasonable levels (high) of information security" (P173) and another said, "I feel I need more education on securing

computer systems. I am too ""trusting"" in what I do" (P262). Others said:

> I wish the university would take a stronger institutional role in this area. Providing a means for easy back-ups and trainings to anyone who uses a computer to make sure they are following safe practices would be very helpful. My efforts to educate those in my department are sometimes dismissed and it would be better if the university were encouraging and training these practices, as well as providing a well-known means for backing up data. (P186)

> I tend to think that ETSU has been too loose with my own information. For months, the site for changing your password, which requires entering your SSN, was not secure; when you checked the locked sign at the lower right hand side you found that their security seal had expired. I got various and sundry answers as to why, including ""not a big deal, don't worry about it."" Suddenly the problem cleared up and they denied that there had ever been a problem when I called to check. C'est la vie. (P399)

> It would be helpful to have a person who would continually update us on what we need to be aware of as far as viruses go. I think OIT does some of that and they actually do a very good job of keeping us up and running at ETSU and yet it might be good to have info passed to us regularly about what not to open on e-mail or what to be watchful for.

> The amount of ""trash"" that gets transmitted through the university system is frightening to me and includes pornography which I really think the OIT department should be able to control for us. (P197)

Specific Issues

The comments revealed three other issues that were of concern to the participants: password management, phishing e-mails, and document management.

Password Management. Some respondents discussed the challenges they faced with password management. Several expressed the following sentiments regarding the challenge of remembering complex and multiple passwords:

> Password management is an ongoing problem issue. With the many distinct systems I interact with, having a unified password is not possible or desirable. As a result I have to keep track of multiple distinct passwords and logins. If passwords are all secure, remembering all of them and the systems they go with is problematic. I find that I have to use a secure program to store my login information in. I wish that other forms of authentication were more readily available so that I wouldn't have to remember all of this information. (P54)

> This issue of frequently changing passwords is an interesting one. I think that there is a serious tension between the mandate for frequent password changes and the injunction against writing down passwords. My observation is that when people are forced to change strong passwords frequently, they must write them down in order to remember them. My choice is to not write my passwords down, but I don't change them frequently. I have multiple strong passwords so that breaking one of these passwords would not compromise all of my logins. (P425)

> There is an inherent trade-off in password security. Strong passwords that are changed frequently are very difficult to remember. This results in more people writing them down, usually on notes in their desk drawer or attached to the computer, a practice that is completely insecure in a setting where others have physical access to the computer. Security protocols need to take into account the very real limits of actual human behavior. (P219)

> Passwords have become burdensome. I am forced to have complex passwords by dozens of different internet sites that I must work with on a daily basis. It is impossible to remember these and equally impossible to keep them totally secure. I review for over a dozen journals, for one example, each journal site has different passwords. And so on. When I stated that I write them down, I mean they are on my Outlook notebook, which I presume is secure, but who knows. (P104)

One commented that recording passwords is not always a bad thing as long as they are secured:

> Recording passwords isn't inherently evil; it depends on how it's done. For example, I have a file on my BlackBerry that records user name and passwords that I rarely use (I'm not worried about those I use routinely, because they are memorized). The BlackBerry file is password protected; since it is a file containing sites my wife might need, she knows the password. Passwords for financial and other confidential systems should be different from those used to sign on to other sites (such as newspaper accounts). (P440)

One commented on the need to share passwords: "I think I understand the concepts of security, but in our department we have to cover for each other from time to time. We are required to share password information and keep everything accessible to each other" (P343).

Phishing E-mails. Some participants commented on their efforts to deal with phishing e-mail. One said, "Whenever I get a phishing message, I usually send a message to OIT, so they can quickly alert ETSU users about the fraudulent e-mail" (P167). Another said, "I also DO NOT open any e-mail that I don't know who sent it" (P356). Others commented on how difficult it is to keep up. Those comments included:

> I believe it's important that I am aware of spam and phishing techniques so that I am not caught off-guard. But I also believe that as the spammers and phishers and hackers get increasingly sophisticated, I'm going to lag far behind in my knowledge of how to maintain security. (P135)
>
> I can easily fend off the older scams--Nigerian money laundering, Pay Pal/bank phishing--but new ones are always coming along. I try to weed them out, but since I receive legitimate e-mails from all over campus and across the nation, I feel vulnerable. Warnings from OIT are much appreciated. (P75)
>
> I wish there was a better system to keep all the junk mail out of our boxes. I never open strange looking e-mail but sometimes it is hard to tell if it is or is not bad when you get all kinds of e-mail from potential students and you wouldn't know their name so you have to open it. (P239)

Document Management and Other Issues. Others expressed concern about a lack of adequate protection for confidential information in some offices. They commented on the failure to secure hard copies of documents that contain confidential information. One questioned the necessity of providing social security numbers to pay parking tickets. Comments included:

> Security has never been an issue in our department, since we all have the same access. Printed material is the only concern. I always make certain that I do not leave any confidential information at the copier. However, if I find that someone has left something at the copier that should not be there, I either try to find the owner or place it in the shred bin. (P170)
>
> Being a part of a big system, I think my role along with everyone else's is extremely important. I don't think there is enough computer security related education given on campus. For instance, I don't think a lot of non-technical people even know how to (or that they should) lock their computer when away from their desk. Also, there is still way too much paper with secure info (like SS#s) floating around campus. I was actually asked for my SS# when paying a parking fine earlier this week. I offered my ID number but refused to give SS#. They were not happy. (P277)

Usefulness of the Survey

Some participants expressed that the survey for this study was helpful in raising their awareness. One said, “After reading this survey, I think I'll change my password!” (P416). Others said, “The questionnaire points out a few things I could do better!” (P360), “I simply hadn't thought about it before. I can see that changing my passwords, deleting unknown e-mails

and making sure a website is secure can help out" (P295) and "I appreciate this survey. Just taking it made me aware of what I might need to change about my behavior" (P247). Another said:

> I know that the user is probably the weakest link in computer security. It depends on the user using safe practices. I try to be a safe user but there are some things that this survey made me aware of that I didn't know existed (ie. the Family Act and passwording specific documents). I will try to find out more about these when I have time.

Quantitative Data Analysis

The survey was completed by 449 respondents. Of the respondents, 401 (89.3%) were from ETSU and 48 (10.7%) were from Milligan College. The survey was sent to all ETSU and Milligan employees with a university or college issued-e-mail account. At the time this survey was distributed, ETSU had 2,178 fulltime employees (ETSU Fact Book, 2007) and Milligan College had about 230 employees (Milligan College 2007-2008 catalog, 2007). Most respondents were fulltime staff (53%) and fulltime faculty (39.2%). Therefore, the return rate was approximately 19%. The highest responses came from the College of Medicine (17.6%). Most respondents were between 50 and 59 years old (37.7%). Table 2 presents detailed information about respondents' positions, work units, and age.

Table 2

Demographics of the ETSU and Milligan College Participants

Participants		*N*	*%*
Position:			
	Full-time faculty	176	39.2
	Adjunct faculty	11	2.4
	Full-time staff	238	53.0
	Part-time staff	6	1.3
	No Response	18	4.0
Work Unit:			
	Biblical, Humane, Social and Scientific Learning, Arts and Sciences	68	15.1
	Business and Technology	47	10.5
	Education	53	11.8
	Medicine	79	17.6
	Nursing and Occupational Therapy	33	7.3
	Public and Allied Health	28	6.2
	Honors College, Continuing Studies, Graduate Studies, Student Affairs, Advancement, Health Sciences	51	11.4
	Academic Affairs	30	6.7
	Business Affairs, Finance and Administration	31	6.9
	No Response	29	6.5
Age Range:			
	20-29	31	6.9
	30-39	83	18.5
	40-49	97	21.7
	50-59	169	37.7
	Over 60	68	15.1
	No Response	1	0.2

Overall, 43% of the respondents had been using computers for over 20 years and only 8% had been using computers for 5 years or less. Most reported that, on average, they spent 3 to 6 hours per day on the computer at work and less than 2 hours on the Internet at work. Table 3 shows the responses.

Table 3

Years of Computer Use, Daily Hours of On-campus Computer Use, and Daily Hours on the Internet

Participants		*N*	*%*
Years of Computer Use:			
	1-5 years	8	1.8
	6-10 years	35	7.8
	11-15 years	95	21.2
	16-20 years	118	26.3
	over 20 years	193	43.0
Average Daily On-Campus Computer Use (not on the Internet):			
	less than an hour	28	6.2
	1-2 hours	90	20.0
	3-4 hours	141	31.4
	5-6 hours	117	26.1
	7-8 hours	63	14.0
	more than 8 hours	10	2.2
Average Daily Hours Spent on the Internet (On-Campus):			
	less than an hour	164	36.5
	1-2 hours	189	42.1
	3-4 hours	62	13.8
	5-6 hours	24	5.3
	7-8 hours	7	1.6
	more than 8 hours	3	0.7

Research Question 3

What are the faculty and staff members computing behaviors reported by the faculty and staff members that either protect or expose them or others to information security attacks?

Descriptive statistics were used to describe ETSU and Milligan College faculty and staff members' computing behaviors that either protect or expose them to information security attacks.

Items 9 through 18 on the survey instrument measured awareness of information security issues and safe computing behaviors. The responses to these items were based on a four-point scale of (1) not aware, (2) somewhat unaware, (3) somewhat aware, and (4) aware. Table 4 presents users' responses to Items 9 through 18.

Table 4

Distribution of Awareness Responses

	Not Aware		Somewhat unaware		Somewhat aware		Aware	
	N	*%*	*N*	*%*	*N*	*%*	*N*	*%*
Aware of the importance of securing passwords			2	0.5	18	4.1	420	95.5
Aware of the impact of responding to phishing e-mails			4	0.9	39	8.8	402	90.3
Aware of the need to update virus protection programs	1	0.2	8	1.8	41	9.2	397	88.8
Aware of virus protection programs	1	0.2	4	0.9	53	11.9	389	87.0
Aware of the impact of viruses			8	1.8	63	14.1	377	84.2
Aware of the importance of backing up files	4	0.9	12	2.7	67	15.0	365	81.5
Aware of vulnerabilities associated with sharing devices	11	2.4	24	5.4	98	22.0	313	70.2
Aware of computer use policies	10	2.2	22	4.9	162	36.1	255	56.8
Aware that encryption can protect confidential information	26	5.8	38	8.5	98	22.0	284	63.7
Aware of FERPA	95	21.2	55	12.3	107	23.9	191	42.6

Most respondents (75.6%) reported that they were aware of most of the awareness items. Most respondents stated that they were aware of the importance of securing passwords (95.5%), the impact of responding to phishing e-mails (90.3%), and the importance of backing up files (81.5%). Seventy percent were aware of vulnerabilities associated with sharing storage devices. Most were aware of the impact viruses can have on computers (84.2%), anti-virus software (87%), and the importance of updating anti-virus software (88.8%). A response of "not aware" was given by less than 6% on all of the awareness items, except one: awareness of FERPA, where 21% reported that they were not aware of FERPA requirements. This item had the lowest 'aware' percentage (42.5%), compared to the other awareness items.

Items 19 through 32 measured the practice of safe computing behaviors. The scale for these items, which indicated the frequency with which the respondents engaged in the stated behaviors, was (1) never, (2) almost never, (3) almost always, and (4) always. Table 5 shows the distribution of responses to the practice items.

Table 5

Distribution of Practice Responses

	Never		Almost never		Almost always		Always	
	N	%	N	%	N	%	N	%
Have antivirus software on home computer(s)	13	3.0	11	2.6	66	15.3	341	79.1
Checks the security of a website before making a financial transaction	12	2.7	24	5.4	102	23.1	304	68.8
Shares password(s) with co-workers	274	61.9	132	29.8	274	6.1	10	2.3
Logs off after using a computer system	15	3.4	51	11.4	104	23.3	277	62.0

Table 5 (continued)

	Never		Almost never		Almost always		Always	
	N	%	N	%	N	%	N	%
Opens emails regardless of not knowing the sender's identity	219	49.1	195	43.7	31	7.0	1	0.2
Updates antivirus software on home computer	20	4.7	30	7.0	130	30.4	248	57.9
Uses a combination of letters, numbers and special characters for passwords	38	8.5	79	17.7	117	26.2	212	47.5
Allows programs to save usernames and passwords for faster access in the future	154	34.8	190	42.9	86	19.4	13	2.9
Writes down password(s)	148	33.1	161	36.0	77	17.2	61	13.6
Back-up my files on reliable media	29	6.5	112	25.1	188	42.2	118	26.2
Install programs from the Internet on work computer	108	24.2	202	45.3	111	24.9	25	5.6
Seek out information security information	54	12.2	154	34.8	145	32.7	90	20.3
Logs off or lock computer before leaving desk	69	15.4	149	33.3	134	30.0	95	21.3
Protects confidential files with passwords	90	20.4	128	29.0	108	24.5	115	26.1

An average of 43.7% indicated that they always practice safe computing behaviors and an average of 31% indicated that they almost always practice safe computing behaviors. Most participants (79.1%) reported that they had antivirus software on their home computer. Approximately 58% stated that they always make sure their antivirus software is updated and

30.4% reported that they almost always keep it updated. Approximately 68% always and 23.1% almost always verify that a website is secure before making a financial transaction. On the subject of passwords, only 47.5% reported that they always use a combination of letters, numbers, and special characters when selecting a password. About 26% stated they almost always use a combination of letters, numbers, and special characters for their passwords. Sixty-nine percent indicated that they never or almost never write down their passwords, and 61.9% indicated that they never share their passwords with coworkers. Approximately 35% reported that they never and 42.9% reported that they almost never allow programs to save their usernames and passwords for faster access in the future.

Almost half (48.8%) reported that they never or almost never log off or lock their computer before leaving their desks temporarily, and 62% reported that they always log off when they finish using their computers. Only 26.2% stated that they always back up their files on reliable media. Approximately 42% stated that they almost always back up their files. Approximately 68% reported that they never or almost never install programs on their work computers as they deemed necessary. Almost half (49.4%) indicated that they always or almost always protect confidential files with passwords. Forty-nine percent indicated that they never open e-mails sent by individuals they do not know. Fifty-three percent reported that they always seek information about information security.

Most respondents (78%) reported that they change their passwords when asked to do so by the system and 7.3% report that they had used the same password for years. Only 7.6% reported that they change their password(s) every 3 months or less. Of the respondents, 278 (61.9%) had wireless internet connection at home and 71.6% of these indicated that their wireless connection was secured. Most respondents (76.8%) indicated that they shred unwanted confidential documents whereas 5.3% indicated that they put the documents in the trash.

Items 36 through 39 measured attitudes towards safe computing behaviors. The scale for these items was (1) strongly disagree, (2) disagree, (3) agree, and (4) strongly disagree. Most respondents (97.1%) indicated that they agreed or strongly agreed that their actions as a user play

a part in securing computer system; 64% agreed that it was fairly easy to engage in secure information security practices and 23.6% strongly agreed. However, 42.9% of the respondents disagreed that it was easy to keep up with new developments related to information security whereas 41% agreed. In addition, 63.4% agreed or strongly agreed that they were reluctant to adapt new technologies until others around them had accepted them. The distribution of the attitudes responses are shown in Table 6.

Table 6

Distribution of Attitude Responses

	Strongly disagree		Disagree		Agree		Strongly Agree	
	N	*%*	*N*	*%*	*N*	*%*	*N*	*%*
User actions affect security	2	0.4	8	1.8	248	55.6	188	42.2
Following secure practices is easy	3	0.7	46	10.3	290	65.2	106	23.8
Keeping up with new information security development is easy	18	4.0	191	42.9	184	41.3	52	11.7
Reluctant to adapt new technologies	83	18.7	199	44.7	149	33.5	14	3.1

Awareness, Practice, and Attitudes Scores

Awareness, practice, and attitudes scores were computed to further analyze the data. The awareness score was obtained by calculating the mean of the responses to Items 9 through 18 on the survey instrument. The practice score was obtained by calculating the mean of the responses from Items 19 through 32 and the attitude scores were obtained by calculating the mean of the responses for Items 36 through 39. Cases that did not have responses to all awareness items, all practice items, or all attitude items were omitted from the calculation. Table 7 shows the means

and standard deviations for the scores.

Table 7

Means and Standard Deviations for Awareness, Practice, and Attitudes Scores

Score	N	M	SD
Awareness	427	3.66	0.36
Attitudes	439	2.83	0.36
Practice	403	2.65	0.32

Research Question 4

In what ways, if any, do attitudes towards information security, awareness of information security issues, and awareness of information security policies make a difference in how faculty and staff members use information technology?

$H_0$4: There is no relationship between information security attitudes score, information security awareness score, and information security practice score. Correlation coefficients were also computed to determine whether faculty and staff members who had positive attitudes toward information security were more aware of safe computing behaviors and also practiced safe computing. The three correlations, as shown in Table 8, were significant at the .02 level, using Bonferroni method to control for Type 1 error across the correlations. Therefore, $H_0$4 was rejected. There was a strong positive correlation between awareness (M = 3.66, SD = 0.36) and practice (M = 2.65, SD = 0.32), a moderate correlation between attitudes (M = 2.83, SD = 0.36) and awareness, and a moderate correlation between attitudes and practice. The results indicated that those with more positive attitudes toward information security tended to be more aware of information security issues and tended to practice safe computing behaviors.

Table 8

Paired Samples Correlations Between Attitude, Awareness, and Practice

Score	Attitudes *r*	Awareness *r*
Awareness	.33[a]*	
Practice	.37[b]*	.52[c]*

Note. [a]N =418, [b]N = 395, [c]N = 385, * p < .02

A paired-samples t-test was conducted to identify differences between attitudes, awareness, and practice of safe computing behaviors. The test was significant at the .02 level, using Bonferroni method to control for Type 1 error across the three pairs. The results indicated that the mean awareness score (M = 3.66, SD = 0.36) was significantly greater than the mean practice score (M = 2.64, SD = 0.31), $t(384) = 59.39$, $p < .01$, $\eta^2 = .90$. The mean awareness score (M = 3.66, SD = 0.36) was also significantly greater than the mean attitudes score (M = 2.84, SD = 0.36), $t(417) = 39.55$, $p < .01$, $\eta^2 = .78$. The mean attitudes score was significantly greater than the mean practice score (M = 2.65, SD = 0.32), $t(394) = 9.27$, $p < .01$, $\eta^2 < .17$. Table 9 shows the results of the paired-samples t-test.

Table 9

Paired Samples t-test of Faculty and Staff Attitudes, Awareness, and Practice Scores

Faculty and Staff		*N*	*M*	*SD*	*T*	*p*	95% Confidence Intervals
Pair 1	Awareness	385	3.66	0.36	59.39	<.01	.98 to 1.04
	Practice		2.64	0.31			
Pair 2	Attitudes	395	2.83	0.36	9.27	<.01	.14 to .22
	Practice		2.65	0.32			
Pair 3	Awareness	418	3.66	0.36	39.55	<.01	.76 to .86
	Attitudes		2.84	0.36			

Note. * p < .02

Because internal consistency estimates of reliability for attitude did not indicate acceptable reliability, the results for the analysis based on the attitude score should be considered unreliable. However, the results from the awareness and practice scores are reliable and it can be concluded that the faculty and staff members appeared to be aware of information security issues and safe computing practices but did not always practice safe computing behaviors. Figure 1 displays the distribution of awareness, attitudes, and practice scores.

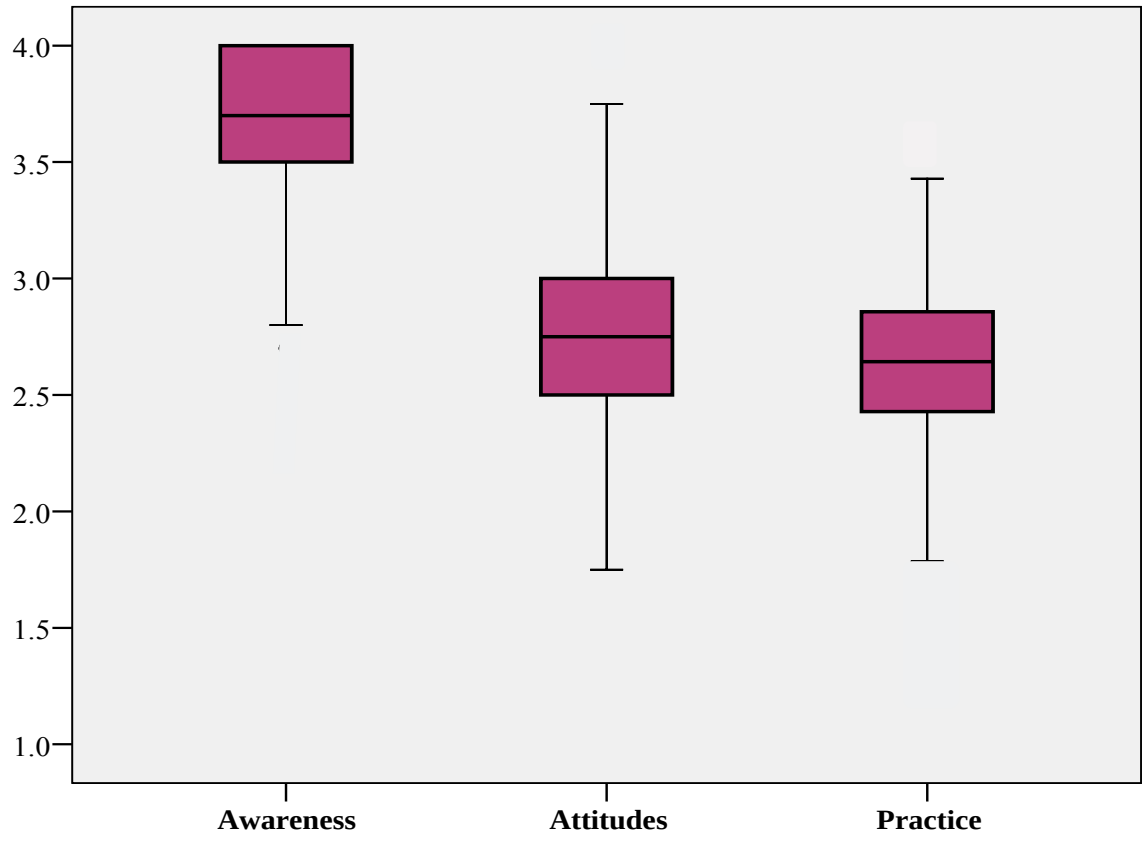

Figure 3. Distribution of Awareness, Attitudes, and Practice Scores

Research Question 5

What differences, if any, exist in information security awareness and practice among faculty and staff members with different demographic characteristics?

$Ho5_1$: There is no difference in information security awareness scores between faculty and staff at ETSU and faculty and staff at Milligan College. A two-way analysis of variance (ANOVA) was conducted to evaluate differences in awareness scores between faculty and staff members at ETSU and faculty and staff members at Milligan College. The ANOVA indicated no significant interaction between institution (ETSU or Milligan College) and position (faculty or staff), $F(1, 405) = 0.15$, $p = .70$, partial $\eta^2 < .01$. Also, there were no significant main effects for institution, $F(1, 405) = 0.69$, $p = .41$, partial $\eta^2 < .01$, and position, $F(1, 405) = 0.03$, $p = .87$, partial $\eta^2 < .01$.

$Ho5_2$: There is no difference in information security practice scores between faculty and staff at ETSU and faculty and staff at Milligan College. A two-way ANOVA was conducted to evaluate differences in practice scores between faculty and staff members at ETSU and faculty and staff members at Milligan College. There were no significant interaction for institution and position, $F(1, 383) = 3.15$, $p = .70$, partial $\eta^2 < .01$. Also, there were no significant main effects for institution, $F(1, 383) = 0.04$, $p = .85$, partial $\eta^2 < .01$, and position, $F(1, 383) = 0.18$, $p = .66$, partial $\eta^2 = .01$. The means and standard deviations for awareness and practice as a function of institution and position are presented in Table 10.

Table 10

Means and Standard Deviations for Awareness and Practice as a Function of Institution and Position

Institution	Position	Awareness			Practice		
		N	*M*	*SD*	*N*	*M*	*SD*
ETSU	Faculty	152	3.64	0.37	143	2.61	0.31
	Staff	212	3.67	0.36	201	2.68	0.31
Milligan College	Faculty	27	3.71	0.34	25	2.69	0.31
	Staff	18	3.69	0.38	18	2.57	0.43

$Ho5_3$: There is no difference in information security awareness scores among those who were 20—29-years old, 30—39-years old, 40—49-years old, 50—59-years old, and over 60-years old. A one-way ANOVA was conducted to evaluate the relationship between age and awareness of information security issues and safe computing practices. The factor variable, age, included five levels: 20—29-years old, 30—39-years old, 40—49-years old, 50—59-years old, and over 60 years-old. The dependent variable was the awareness score. The ANOVA was not significant, $F(4, 421) = 1.07$, $p = .32$, partial $\eta^2 = .01$. Therefore, $Ho5_3$ was retained.

$Ho5_4$: There is no difference in information security practice scores among those who are 20—29-years old, 30—39-years old, 40—49-years old, 50—59-years old, and over 60-years old. A one-way ANOVA was conducted to evaluate the relationship between age and practice of safe computing behaviors. The dependent variable was the practice score. The ANOVA was not significant, $F(4, 397) = 1.07$, $p = .38$, partial $\eta^2 = .01$. Therefore, $Ho5_4$ was retained. The means and standard deviations for awareness and practice as a function of age are shown in Table 11.

Table 11

Means and Standard Deviations for Awareness and Practice as a Function of Age

Age	Awareness		Practice	
	M	*SD*	*M*	*SD*
20—29 years old	3.59	0.07	2.62	0.06
30—39 years old	3.61	0.04	2.60	0.04
40—49 years old	3.69	0.04	2.69	0.03
50—59 years old	3.66	0.03	2.65	0.03
Over 60 years old	3.71	0.05	2.65	0.04

$Ho5_5$: There is no difference in information security awareness scores among those who had 15 years or less, 16—20 years, and over 20 years of computer use. A one-way ANOVA was conducted to evaluate the relationship between years of computer use and awareness of information security issues and safe computing practices. The ANOVA was significant, $F(2, 418) = 9.45$, $p < .01$, partial $\eta^2 = .04$. Therefore, $H5_5$ was rejected. The effect size, as assessed by η^2, was small, with years of computer use accounting for 4% of variance of the awareness scores.

Because the overall *F* was significant, follow-up tests were conducted to evaluate pairwise differences among means of the three groups. The Dunnett's C procedure was selected for multiple comparisons because equal variances were not assumed. There was a significant difference in means between the group that had used computers for over 20 years and the groups that had used computers for 16—20 years, and 15 years or less. However, there was no significant difference between the group that had used computers for 16—20 years and the group that had used computers for 15 years or less. The group that had used computers for over 20 years tended to be more aware of information security issues and safe computing practices. The 95% confidence intervals, as well as means and standard deviations for awareness as a function

of years of computer use, are reported in Table 12.

Table 12

Means and Standard Deviations With 95% Confidence Intervals of Awareness Pairwise Differences

Years of Computer Use	N	*M*	*SD*	15 years or less	16—20 years
15 years or less	126	3.57	0.42		
16—20 years	110	3.62	0.34	-.07 to .16	
Over 20 years	185	3.74	0.61	.65 to .27*	.03 to .22*

Note. * The mean difference is significant at the .05 level using Dunnett's C procedure

$Ho5_6$: There is no difference in information security practice scores among those who had 15 years or less, 16—20 years, and over 20 years of computer use. A one-way ANOVA was conducted to evaluate the relationship between years of computer use and practice of safe computing behaviors. The ANOVA was significant, $F(2, 394) = 3.20$, $p < .04$. Therefore, $H5_6$ was rejected. The effect size, as assessed by η^2, was small, with years of computer use accounting for 2% of variance of the practice scores.

Because the overall *F* was significant, follow-up tests were conducted to evaluate pairwise differences among means of the three groups. The LSD procedure was selected for multiple comparisons because equal variances were assumed. The results indicated a significant difference in means between the groups. The group that had used computers for over 20 years practiced safe computing habits more than those who had used computers for 16—20 years and less than 15 years. The 95% confidence intervals, as well as means and standard deviations for practice as a function of years of computer use, are shown in Table 13.

Table 13

Means and Standard Deviations With 95% Confidence Intervals of Practice Pairwise Differences

Years of Computer Use	N	*M*	*SD*	15 years or less	16-20 years
15 years or less	116	2.61	0.35		
16—20 years	107	2.61	0.31	-.09 to .07	
Over 20 years	174	2.69	0.30	.002 to .15*	.009 to .16*

Note. * The mean difference is significant at the .05 level using the LSD procedure

$Ho5_7$: There is no difference in awareness and practice scores among those who spent a daily average of 2 hours or less, 3—4 hours, 5—6 hours, and 7 or more hours on the computer (not on the Internet). A one-way multivariate analysis (MANOVA) was computed to determine whether there was a relationship between daily computer use (2 hours or less, 3—4 hours, 5—6 hours, and 7 or more hours), and awareness and practice of safe computing behaviors. There were no significant differences among the four groups on the dependent variables, Wilks's Lambda = .97, $F(6, 712) = 1.58$, $p = .15$, partial $\eta^2 = .01$. Therefore, $H5_7$ was retained. Table 14 shows the means and standard deviations on the dependent variables for the four groups.

Table 14

Daily Computer Use Groups' Awareness and Practice Means and Standard Deviations

Daily Computer Use	N	Awareness		Practice	
		M	*SD*	*M*	*SD*
2 hours or less	76	3.60	0.41	2.58	0.37
3—4 hours	127	3.64	0.38	2.64	0.31
5—6 hours	93	3.70	0.31	2.67	0.31
7 or more hours	65	3.67	0.30	2.70	0.29

$Ho5_8$: There is no difference in awareness and practice scores among those who spent a daily average of less than 1 hour, 1—2 hours, and 3 or more hours on the Internet. A one-way MANOVA was conducted to determine whether there was a relationship between daily Internet use (less than 1 hour, 1—2 hours, and 3 or more hours), and awareness and practice of safe computing behaviors. There were no significant differences among the three groups on the dependent variables, Wilks's Lambda = .99, $F(4, 762) = 1.40$, $p = .23$, partial $\eta^2 < .01$. Therefore, $Ho5_8$ was retained. Table 15 shows the means and standard deviations on the dependent variables for the four groups.

Table 15

Daily Internet Use Groups' Awareness and Practice Means and Standard Deviations

Daily Internet Use	N	Awareness		Practice	
		M	*SD*	*M*	*SD*
Less than 1 hour	139	3.65	0.37	2.62	0.32
1—2 hours	167	3.63	0.36	2.65	0.31
3 or more hours	79	3.72	0.34	2.69	0.35

Summary

Chapter 4 presented qualitative and quantitative analyses of interviews and survey data collected about ETSU and Milligan faculty and staff members' computing behaviors. The analysis involved analyzing faculty and staff members' computing behaviors as perceived by IT professionals and by the faculty and staff themselves.

CHAPTER 5

SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

The purpose of the study was to explore perceived faculty and staff members' behaviors that either protect or expose them to information security attacks. The study explored ETSU and Milligan College faculty and staff members' computing behaviors. Data collected from interviews with IT professionals and an online survey were analyzed to understand the faculty and staff members' computing behaviors. This chapter concludes the research. It summarizes findings and conclusions, recommendations for practice, and recommendations for future research.

Findings Related to the Study's Five Research Questions

Research Question 1

What are the computing behaviors of faculty and staff members that either protect or expose them or others to information security attacks as observed by information technology professionals?

The IT professionals who participated in this study reported that password mismanagement was the major problem they encountered with authorized users. They stated that faculty and staff members often shared their passwords with colleagues and student workers. They reported that faculty and staff members tended to write down their passwords and to choose weak passwords. They also reported that some authorized users did not always log off their computers. Some participants attributed these behaviors to users' lax attitudes towards information security and lack of understanding of the impact of their behaviors. One IT professional stated that users tend to write down passwords that are too complex to remember.

IT professionals said they believed that faculty and staff members routinely fail to secure the contents of their portable storage devices such as USB flash drives. Even though users may be aware of these device's vulnerabilities, they did not know how to secure them, and encryption

was not yet seen as a feasible strategy for securing data. ETSU plans to invest in data encryption products in the future. In the meantime, ETSU IT professionals recommended discouraging faculty and staff members from storing confidential information on portable storage devices. Some also reported that they had seen hard copies of confidential documents placed in plain sight for anyone to observe.

ETSU IT participants said they believed that most users used a shredder or confidential document disposal bins in some ETSU offices to dispose of sensitive documents. However, it seemed there were no institution-wide policies addressing this issue.

Both institutions provide users with storage on campus servers and do frequent backups on these servers. However, participants reported incidents of permanent data loss because of accidental data deletion or equipment failure involving data that were neither stored on network servers nor backed-up. In general, faculty and staff members appeared to use their server space for storage.

ETSU and Milligan IT professionals reported that they rely on special applications rather than user vigilance to manage malware. However, they also noted that faculty and staff members were aware of the impact of malware.

Participants reported that phishing e-mails were concerns. They said they believed that users were generally aware of the threat and tended not to reply to phishing e-mails. The ETSU and Milligan IT departments use filtering software to screen incoming e-mail. This software prevented most, but not all, phishing attempts from reaching users' inboxes. Phishing techniques, however, were becoming more sophisticated, and some people were falling victim to these attempts. IT professionals reported that they tried to educate users to recognize phishing e-mails and alert users to especially insidious phishing attempts that evade the filters.

Participants expressed concerns about the violation of ethics of computing by some faculty and staff members, although that was not the study's focus. They stated that FERPA compliance was a management issue and the Registrar's Office was responsible for enforcing FERPA.

It appeared that the consensus among the IT professionals was that even though faculty and staff were aware of information security issues, they tended not to practice safe computing behaviors until an unfortunate incident occurred. Unfortunate events that were close to home tended to shake users into practicing safe computing behaviors.

The main point of disagreement between ETSU's and Milligan's IT professionals involved the granting of administrative privileges to faculty and staff members. ETSU participants, unlike Milligan participants, were in favor of limiting privileges for faculty and staff members to those who needed them. This difference might be because Milligan is a small college where the IT personnel have the advantage of knowing every faculty and staff member. ETSU, on the other hand, has over 2,000 employees and it is difficult for ETSU IT personnel to know all of them personally. Also, Milligan, as a private and religious college, is free to enforce a stricter code of conduct than is ETSU.

Neither ETSU nor Milligan offered an intensive orientation in information security for new employees, although they made these employees aware of the institutions' computing policies. However, both institutions regularly offered voluntary information security training and used several modes of communication to inform users about information security issues.

Research Question 2

What are the faculty and staff members' attitudes toward the role they play in securing computer systems as reported by the faculty and staff members?

ETSU and Milligan faculty and staff members tend to perceive that their computing behaviors could have an impact on the security of computer systems. Most reported that they had a responsibility in securing computer systems. It appears there were four groups of users at ETSU and Milligan College. The first group indicated that they were very aware of information security issues and made every effort to practice safe computing behaviors. The second group indicated that they understood their responsibilities and information security issues and were willing to practice safe computing behaviors but needed more education to do that. The third

were aware of their responsibilities and understood information security issues but did not take that responsibility seriously or they simply did not care. They put all the responsibility on the IT departments. Some stated that they had too many responsibilities to focus on safe computing behaviors and relied on IT for computer security. The fourth avoided using computers as much as possible because they did not like using computers or because they simply did not think they were equipped to use computers securely.

Some assumed responsibility for acting as role models and for educating others about secure computing. Most users stated that their IT departments played a major role in securing computer systems. The IT responsibilities included educating users and providing technical solutions.

Users discussed password management, phishing e-mails, and document management in their observations about secure computing practices. They tended to agree that managing passwords was a challenge for them. They indicated that it was challenging to remember complex passwords, especially multiple complex passwords. One user argued that there was an occasional need to share passwords because of the nature of work. Users stated that they were diligent about fending off phishing attempts. Some stated that they did not open suspicious e-mails. However, users also acknowledged that it was becoming difficult to distinguish some phishing e-mails. In those cases, some notified their IT departments. Some users expressed concern that hard copies of confidential information were not adequately protected in some offices. In some instances, confidential information was available to those who did not need it to perform their duties. Finally, some reported that participating in this study helped them recognize some computing behaviors they needed to correct.

Research Question 3

What are the faculty and staff members' computing behaviors that either protect or expose them or others to information security attacks as reported by the faculty and staff members?

Most ETSU and Milligan faculty and staff members (75.6%) indicated that they were aware of information security related issues. However, only 42.6% reported that they were aware of the FERPA requirements; 21.2% reported that they were not aware of FERPA requirements. Only 56.8% were aware of computer use policies at their institutions although 36% indicated that they were somewhat aware of the policies.

An average of 43.7% indicated that they always practiced safe computing behaviors and an average of 31% indicated that they almost always practiced safe computing behaviors. Most respondents (78%) reported that they change their passwords when asked to do so by the system and only 7.6% reported that they change their password(s) every 3 months or less. Most (71.6%) of those who had wireless Internet connection at home reported that their wireless connection was secured. Most respondents (76.8%) also indicated that they shredded unwanted confidential documents.

Research Question 4

In what ways, if any, do attitudes towards information security, awareness of potential information security issues, and awareness of information security policies make a difference in how faculty and staff members use information technology?

The results from a paired-samples t-test showed that the faculty and staff members' awareness of safe computing behaviors exceeded the extent to which they practiced those behaviors. Significant positive correlations were observed between attitudes, awareness, and practice of safe computing behaviors. The correlation between attitude and awareness together with the correlation between attitude and practice is not reliable because the instrument review failed to establish this aspect of the instrument's reliability. Nonetheless, the results showed that the more aware the faculty and staff members were, the more they practiced safe computing behaviors.

Research Question 5

What differences, if any, exist in information security awareness and practice among faculty and staff members with different demographic characteristics?

The analysis of the data indicated that there were no significant differences in awareness of information security issues between faculty and staff members at ETSU and Milligan College. The computing behaviors of ETSU faculty and staff and the computing behaviors of Milligan faculty and staff members were similar. Also, the computing behaviors of ETSU and Milligan faculty members were similar to the computing behaviors of ETSU and Milligan staff members.

There were no significant differences in awareness of information security issues and practices among the five age groups (20—29-years old, 30—39-years old, 40—49-years old, 50—59-years old, and over 60-years old). Also, there were no significant differences in safe computing practices among these age groups.

The results indicated that faculty and staff members who had used computers for over 20 years tended to be more aware of information security issues and tended to practice safer computing behaviors than did those who had used computers for 20 years or less. However, there was no relationship between average daily computer use (2 hours or less, 3—4 hours, 5—6 hours, and 7 or more hours) and awareness and practice of safe computing behaviors. Also, there were no significant differences in awareness of information security issues and practice of safe computing habits among those who spent less than 1 hour, 1-2 hours, and 3 or more hours on the Internet.

Findings in Relation to Literature Review

This study indicated that faculty and staff members at the two participating institutions were aware of information security issues and safe computing practices. The findings support what was found by Aytes and Connoly (2004) and Furnel (2005). However, the faculty and staff did not always practice safe computing behaviors as much as they were aware of information security issues and safe computing behaviors.

Fishbein and Ajzen (1975), Davis (1986), and Dillon and Morris (1996) argued that attitudes towards a behavior influences a person's behaviors. The results from this study indicated that this seemed to be the case with ETSU and Milligan faculty and staff members. However, the results were not reliable because the internal consistency of the attitude measure was unacceptable.

In 2003, the University of Pennsylvania identified weak passwords as the most significant threat to the security of its computer systems (Foster, 2004). ETSU conducted a similar evaluation and found that this was true for ETSU as well. Consequently, ETSU implemented a complex password policy.

The literature review identified a study from 2006 that found users were not aware of the need to secure wireless connections (Barile). This study determined that most faculty and staff members at ETSU and Milligan College had secured their wireless connection at home.

Ashe (2004) and Simons (2005) indicated that ETSU's tolerance for decentralized management of information resources helped to create situations where systems were managed by users who failed to properly secure their systems. This situation seems to persist at ETSU and Milligan because faculty and staff members had administrative privileges on their office computers. ETSU and Milligan also seem to have no standard policies for disposing of sensitive documents, although ETSU was working on a policy to manage portable devices.

Best practices in institutional computer security include instituting and enforcing information security policies and training users to practice safe computing behaviors (Anderson, 2001; Bishop, 2005; Camp et al., 2007; Canavan, 2001; Conklin et al., 2004). ETSU and Milligan College have information security policies, but failed to enforce them consistently. They also offer training programs, although they were voluntary.

Conclusions

The following conclusions can be drawn from these findings:

1. ETSU and Milligan faculty and staff members are aware of information security issues and safe computing practices although they do not always practice safe computing behaviors to the same extent as they are aware.
2. There were no significant differences between faculty and staff members with different demographic characteristics except for years of computer use. Those who had used computers for more than 20 years were significantly more aware of information security issues and practiced safe computing behaviors more than those who had used computers for fewer years.
3. Password management continues to challenge users and IT departments.
4. Security applications such as antivirus programs have been instrumental in managing malware risks.
5. Faculty and staff members have learned to deal with phishing e-mails. However, phishing attempts continued to be a challenge as the creators were becoming more sophisticated in their attempts.
6. Both institutions have training programs but attendance was not required. The majority of faculty and staff members would like to have more training and support from their IT departments.
7. Although FERPA was one of the major acts that govern the protection of students' records, faculty and staff at ETSU and Milligan appear to be unaware of FERPA guidelines.
8. IT professionals were concerned with unethical and illegal behaviors that some users engaged in while using ETSU and Milligan College information resources.

Recommendations for Practice

The following are recommendations for administrators and IT professionals based on the findings of this study:

1. The complex password policy recently instituted at ETSU should be commended. The

only suggestion I can offer is that more instructions should be available to guide users in selecting passwords that are complex but also easy to remember, thereby removing the need to write them down.

2. The findings revealed that there currently is no intensive information security training for new employees. It will be worthwhile to offer a new employee orientation that focuses on introducing new employees to information security resources available for them. Intensive information security training should be considered for employees who work with sensitive information.
3. ETSU was in the process of exploring ways to manage portable devices. That process should continue. Milligan, as well, should explore this process.
4. Faculty and staff members are encouraged not to store confidential information on portable devices unless the data on the device are encrypted.
5. Faculty and staff members should be encouraged to take time to read their institution's computer use polices.
6. Faculty and staff members should be encouraged to take time to read the FERPA guidelines.

Recommendations for Further Research

The following recommendations for further research are based on the findings of this study.

1. A study should be extended to include other institutions of different sizes and in different parts of the country and world.
2. A more extensive qualitative study should be conducted to understand the disparities between awareness and practice and also to understand faculty and staff attitudes towards the practice of safe computing behaviors.
3. This study determined that there were significant differences between faculty and staff members who had used computers for over 20 years and those who had used computers for 20 years or less. The Internet and personal computers became popular

4. There is need to develop a quantitative instrument that measures attitudes towards information security that can be used to assess the impact of attitudes on secure computing behaviors.
5. A study of faculty and staff members' attitudes towards ethics of computing would be informative. The study could provide information to help IT professionals and administrators address the ethical and legal concerns raised in this study.

REFERENCES

Acceptable Use Policy. (2000). Retrieved from http://www.etsu.edu/oit/ppp /aup/default.asp

Anderson, R. J. (2001). *Security engineering: A guide to building dependable distributed systems.* New York: Wiley.

Ary, D., Jacobs, L. C., & Razavieh, A. (2002). *Introduction to research in education* (6th ed.). Belmont, CA: Wadsworth Thomas.

Ashe, J. P. (2004). *A vulnerability assessment of the East Tennessee State University administrative computer network.* Unpublished master's thesis, East Tennessee State University, Johnson City.

Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing, 16*(3), p. 22-40.

Babbie, E. (2000). *The practice of social research* (9th ed.). Belmont, CA: Wadsworth Thomas.

Barile, I. (2006). *Protecting your pc*. Boston: Charles River Media.

Bishop, M. (2005). *Introduction to computer security.* Boston: Pearson.

Bosworth, S., & Jacobson, R. V. (2002). Brief history and mission of information system security. In S. Bosworth & M. E. Kabay (Eds.), *Computer security handbook* (4th ed.) (pp. 1.1-1.13). New York: John Wiley & Sons.

Camp, J. S., Deblois, P. B., & the EDUCAUSE Current Issues Committee. (2007). *Current issues survey report, 2007. EDUCAUSE Review, 30*. Retrieved from http://www.educause.edu/ir/library/pdf/eqm0723.pdf

Campus-Wide Password Policy Change. (2008). Retrieved from http://www.etsu.edu/oit/acrobat/strong_password_policy_2007.pdf

Canavan, J. E. (2001). *Fundamentals of network security*. Norwood, MA: Artech House.

Caruso, J. B. (2006). *Safeguarding the tower: IT security in higher education 2006 (Key Findings)*. EDUCAUSE Center for Applied Research. Retrieved from http://connect.educause.edu/library/abstract/SafeguardingtheTower/41170

Cate, F. H. (2006). The privacy and security policy vacuum in higher education. *Educause Review, 41*, 19-28. Retrieved from http://www.educause.edu/ir/library /pdf/erm0651.pdf

CDW Government. (2006). *CDW-G higher education IT security report card 2006*. Retrieved from http://newsroom.cdwg.com/features/HEITSecurityReportCard10-10-06.pdf

Conklin, W. A., White, G. B., Cothren, C., Williams, D., & Davis, R. L. (2004). *Principles of computer security: Security+ and beyond*. Boston: McGraw-Hill.

Crews, K. D. (2006). Distance education and the TEACH act. *American Library Association*. Retrieved from http://www.ala.org/ala/washoff/WOissues/copyrightb/distanceed /distanceeducation.htm

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: theory and results*. Unpublished doctoral dissertation, Massachusetts Institute of Technology, Cambridge.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*, 318-340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science 35*, 982-1003.

Dillon, A., & Morris, M. (1996). User acceptance of new information technology: Theories and models. In M. Williams (Ed.), *Annual review of information science and technology, 31*(pp. 3-32). Medford, NJ: Information Today.

Elliott, R., Young, M. O., Collins, V. D., Frawley, D., & Temares, L. (1991). Retrieved from the Educause Center for Applied Research Web site: http://www.educause.edu/ir/library /pdf/PUB3005.pdf

ETSU enrollment surpasses 13,000 for first time. (2007). Retrieved September 20, 2007, from http://www.etsu.edu/calendars/calendars_news.asp?EventID=6381

ETSU fact book. (2007). Retrieved from http://www.etsu.edu/iep/07FB /07TOC.htm

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.

Foster, A. (2005, December 16). When databases leak. [Electronic Version]. *The Chronicle of Higher Education,* A31-A34.

Foster, A. L. (2004, December 17). Institutions spend more to defend their networks, a chronicle survey finds [Electronic Version]. *The Chronicle of Higher Education,* A1.

Glasser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory.* Chicago: Aldine.

Hawkins, B. L., & Rudy, J. A. ,(2006). *Fiscal year 2005 summary report.* Retrieved from http://www.educause.edu/ir/library/pdf/pub8003.pdf

Holub, T. (2003). College student records: Legal issues, privacy, and security concerns. *Eric Digest*, 1-6.

Information integrity defined. (n.d.). Retrieved from http://www.infogix.com/ii_defined

Information technology faculty and staff help pages. (n.d.). Retrieved from

http://www.milligan.edu/it/Faculty_Staff_Help.htm

Information technology code of ethics. (2003). Retrieved from http://www.etsu.edu/humanres/ppp/PPP-44.htm

Jaeger, P. T., McClure, C. R., Bertot, J. C., & Snead, J. T. (2004). The USA patriot act, the foreign intelligence surveillance act, and information policy research in libraries: Issues, impacts, and questions for libraries and researchers. *Library Quarterly*, *74,* 99-121.

Kissel, R., Scholl, M., Skolochenko, S., & Li, X. (2006). *Guidelines for media sanitization*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

Kvavik, R. B., Voloudakis, J., Caruso, J. B., Katz, R. N., King, P., & Pirani, J. A. (2003). Information technology security: Governance, strategy, and practice in higher education. *Educause Center for Applied Research*. Retrieved from http://www.educause.edu/ers0305.

Latest Information on Veterans Affairs Data Security. (n.d.). Retrieved from http://www.firstgov.gov/veteransinfo.shtml

McMillan, J. H., & Schumacher, S. (2006). *Research in education: Evidence-based inquiry* (6th ed.). Boston: Allyn and Bacon.

Merrian, S. B. (1998). *Qualitative research and case study applications in education* (2nd ed.). San Francisco: Jossey-Bass.

Milligan college catalog 2007 – 2008. (2007). Retrieved from http://www.milligan.edu/academics/pdf/Catalog.pdf

Milligan college computer use policy. (n.d.). Retrieved from http://www.milligan.edu/it/Policies.htm

Neuman, W. L. (1997). *Social research methods: Qualitative and quantitative qpproaches* (3rd ed.). Boston: Allyn and Bacon.

Office of Information Technology. (n.d). Retrieved from http://www.etsu.edu/oit

Rosenberg, R. S. (2004). *The social impact of computers* (3rd ed.). Boston: Elsevier Academic Press.

Ryan, J. E. (2006). A comparison of information security trends between formal and informal environments. Retrieved April 20, 2007, from *ProQuest Digital Dissertations* database. (Publication No. AAT 3225287)

Salomon, K. D., Cassat, P. C., & Thibeau, B. E. (2003). *IT security for higher education: A legal perspective.* Retrieved from http://www.educause.edu/ir/library/pdf/CSD2746.pdf

Shih, H. (2004). An empirical study on predicting user acceptance of e-shopping on the web.

Information & Management 41, 351-368.

Simons, W. R. (2005). *The challenges of network security remediation at a regional university.* Unpublished Master's thesis. East Tennessee State University, Johnson City.

Smith, J., & Frisby, J. (2004). A five-step plan for comprehensive information security and privacy [Electronic Version]. *Bank Accounting and Finance, 17*, 31-37.

Snyder, A. L. (2006). Mixed-method designs. In J. H. McMillan & S. Schumacher (Eds.), *Research in education: Evidence-based inquiry* (pp. 400-420). Boston: Allyn and Bacon.

Staton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors [Electronic Version]. *Computer & Security, 24*, 124-133.

Stewart, J. M., Tittel, E., & Chapple, M. (2005). *CISSP: Certified information system security professional study guide* (2nd ed.). San Francisco: Sybex.

Symantec. (2007, March 17). *Symantec internet security threat report: Trends for June-December 2006*. Retrieved from http://www.symantec.com/content/en/us/about/media/ISTR_XI_Global_FINAL.pdf

Taylor, S., & Todd, P. (1995). Assessing IT usage: The role of prior experience. *MIS Quarterly,19*, 561-570.

Thomson, K., & Solms, R. (2005). Information security obedience: A definition [Electronic Version]. *Computer & Security 24,* 69-75.

Trcek, D., Trobec, R., Pavesic, N., & Tasic, J. F. (2007). Information systems security and human behavior[Electronic Version]. *Behaviour & Information Technology, 26,* 133-118.

University of California, Los Angeles. (2006, December 12). *UCLA warns of unauthorized access to restricted database*. Retrieved December 14, 2006, from http://www.newsroom.ucla.edu/page.asp?RelNum=7571.

Wikipedia (n. d.). *Computer virus.* Retrieved from http://en.wikipedia.org/wiki/Computer_virus

Wikipedia (n. d.). *USB flash drive.* Retrieved from http://en.wikipedia.org/wiki/USB_flash_drive

Young, J. R. (2005, November 18). User error, not hackers, is top source of campus computer problems, survey finds [Electronic Version]. *The Chronicle of Higher Education,* A36.

APPENDICES

APPENDIX A

Interview Guide

1. How long have you worked in this Department?
2. How do you keep users informed about information security issues?
3. What kind of training programs do you offer to faculty and staff members to help them use information technology securely?
4. From your experience, what are the computing behaviors of faculty and staff at your institution that either expose or protect them from information security attacks, especially in the following areas?
    a. Password management
    b. Data storage devices and document management
    c. Data back-up management
    d. Knowledge of Federal and State information security laws - FERPA
    e. Defense against malware
    f. Defense against phishing email

APPENDIX B

Information Security Survey Instrument

Demographic Information

1. Please select your institution
   O East Tennessee State University
   O Milligan College

2. Please indicate your gender
   O Female
   O Male

3. Please select the range that reflect your current age
   O below 20
   O 20 – 24
   O 25 – 29
   O 30 – 34
   O 35 – 39
   O 40 – 44
   O 45 – 49
   O 50 – 54
   O 55 – 59
   O 60 – 64
   O over 64

4. Please select the range that best indicate the number of years you have used computers
   O less than 1 year
   O 1 – 5 years
   O 6 – 10 years
   O 11 – 15 years
   O 16 – 20 years
   O over 20 years

5. Please indicate your current job classification
   O Full-time faculty
   O Adjunct faculty
   O Full-time staff
   O Part-time staff
   O Other

6. In which college or unit do you work?

ETSU	Milligan College
O Arts and Sciences	O Biblical Learning
O Business and Technology	O Business
O Education	O Education
O Medicine	O Humane Learning
O Nursing	O Nursing
O Public and Allied Health	O Occupational Therapy
O Honors College	O Performing, Visual, and Communicative Arts
O School of Continuing Studies	O Scientific Learning
O School of Graduate Studies	O Social Learning
O Academic Affairs	
O Finance and Administration	
O Health Sciences	
O Student Affairs	
O University Advancement	

On-campus computer use

7. Please select a range that best indicates your average daily hours of on-campus computer use (not on the Internet)
    O less than 1 hour
    O 1 – 2 hours
    O 3 – 4 hours
    O 5 – 6 hours
    O 7 – 8 hours
    O more than 8 hours

8. Please select a range that best indicates your average daily hours you spend on the Internet on-campus
    O less than 1 hour
    O 1 – 2 hours
    O 3 – 4 hours
    O 5 – 6 hours
    O 7 – 8 hours
    O more than 8 hours

Please answer the following questions according to your computer use at work, unless otherwise specified.

Information Security Awareness

With respect to information technology and its security, I am aware…	not aware	somewhat unaware	somewhat aware	aware
9. of the requirements and expectations of the computer use policies at my institution.	O	O	O	O
10. of the impact that a virus can have on my computer system.	O	O	O	O
11. that virus protection software can identify and remove viruses.	O	O	O	O
12. that virus protection software requires frequent updates.	O	O	O	O
13. that I should keep my passwords secure.	O	O	O	O
14. of the requirements of the Family Educational Rights and Privacy Act (FERPA).	O	O	O	O
15. of the impact of responding to phishing emails (e.g. unsolicited emails asking for your bank information).	O	O	O	O
16. that it is important to back-up my files	O	O	O	O
17. that encryption can prevent unauthorized access to confidential information.	O	O	O	O
18. of the vulnerabilities associated with sharing devices such as files and drives.	O	O	O	O

Information Security Practice

To what extent do you do the following:	never	almost never	almost always	always
19. I log off or lock my computer before I step away from my desk?	O	O	O	O
20. I log off when I finish using a computer system.	O	O	O	O
21. When choosing a password, I use a	O	O	O	O

To what extent do you do the following:	never	almost never	almost always	always
combination of letters, numbers and special characters.				
22. I write down my password(s).	O	O	O	O
23. I share my password(s) with my co-workers.	O	O	O	O
24. I back-up my files on reliable media.	O	O	O	O
25. I have antivirus software on my home computer(s).	O	O	O	O
26. I keep the antivirus software on my home computer updated.	O	O	O	O
27. I allow programs to save my usernames and passwords for faster access in the future.	O	O	O	O
28. I download and install programs from the internet as I deem necessary on my work computer.	O	O	O	O
29. I protect confidential files with passwords.	O	O	O	O
30. I check whether a website is secure or not before making a financial transaction over the internet.	O	O	O	O
31. I seek out information about information security	O	O	O	O
32. I open emails regardless of not knowing the sender's identity	O	O	O	O

33. My wireless Internet connection at home is
    - O secured
    - O not secured
    - O I don't know
    - O I don't have wireless connection

34. I change my password(s)
    - O when I am asked to (by the system)
    - O every month
    - O every three months or less
    - O every six months or less
    - O Every 12 months or less
    - O I have used the same password(s) for years

35. When disposing confidential documents such as an official class roster
    - O I usually place them in the trashcan.
    - O I usually tear up the documents and place them in the trashcan.
    - O I usually use a shredder.

Attitude towards Information Security Awareness and Practice

With respect to information technology and its security, …	strongly disagree	disagree	agree	strongly agree
36. I think it is fairly easy to follow secure information security practices.	O	O	O	O
37. I believe my actions as a user play a part in securing computer systems.	O	O	O	O
38. I find it easy to keep up with new developments related to information security.	O	O	O	O
39. I am reluctant to adapt new technologies until I see the majority of the people around me accept them.	O	O	O	O

40. In the space below, write a few comments about your feelings about the role you play in securing computer systems.

APPENDIX C

Informed Consent Document

EAST TENNESSEE STATE UNIVERSITY
VETERANS AFFAIRS MEDICAL CENTER
INSTITUTIONAL REVIEW BOARD
INFORMED CONSENT DOCUMENT (ICD)
FOR PROSPECTIVE RESEARCH INTENDED FOR REVIEW

This Informed Consent will explain about being a participant in a research study. It is important that you read this material carefully and then decide if you wish to be a volunteer.

PURPOSE:

This study is dissertation study required to complete my doctorate degree. The objective of this study is to identify faculty and staff habits that make academic institutions either more or less vulnerable to information security attacks.

DURATION

It will take 30 - 60 minutes of your time to complete the interview.

PROCEDURES

I will ask you questions regarding information security. The interview will be recorded and I will also take notes during the course of the interview.

ALTERNATIVE PROCEDURES/TREATMENTS

There are no alternative procedures except not to participate.

POSSIBLE RISKS/DISCOMFORTS

There are no foreseeable risks associated with this study.

POSSIBLE BENEFITS

The results of the study may provide useful information that you can use to help faculty and staff use computers securely.

VOLUNTARY PARTICIPATION

Participation in this research experiment is voluntary. You may refuse to participate. You can quit at any time. If you quit or refuse to participate, the benefits to which you are otherwise entitled will not be affected. You may quit by calling me, Chiwaraidzo Judith Nyabando, at

(423) 433-3459. You will be told immediately if any of the results of the study should reasonably be expected to make you change your mind about staying in the study.

CONTACT FOR QUESTIONS

If you have any questions, problems or research-related medical problems at any time, you may call me, Chiwaraidzo Judith Nyabando, at (423) 433-3459, or Dr. Jasmine Renner at (423) 439-7629. You may call the Chairman of the Institutional Review Board at (423) 439-6054 for any questions you may have about your rights as a research subject. If you have any questions or concerns about the research and want to talk to someone independent of the research team or you can't reach the study staff, you may call an IRB Coordinator at (423) 439-6055 or (423) 439-6002.

CONFIDENTIALITY

Every attempt will be made to see that your study results are kept confidential. A copy of the records from this study will be stored in Warf-Pickel, room 501 for at least 5 years after the end of this research. The results of this study may be published and/or presented at meetings without naming you as a subject. Although your rights and privacy will be maintained, the Secretary of the Department of Health and Human Services, ETSU, and personnel particular to this research, members of my dissertation committee have access to the study records. Your records will be kept completely confidential according to current legal requirements. They will not be revealed unless required by law, or as noted above.

By signing below, you confirm that you have read or had this document read to you. You will be given a signed copy of this informed consent document. You have been given the chance to ask questions and to discuss your participation with the investigator. You freely and voluntarily choose to be in this research project.

SIGNATURE OF PARTICIPANT DATE

PRINTED NAME OF PARTICIPANT DATE

SIGNATURE OF INVESTIGATOR DATE

SIGNATURE OF WITNESS (if applicable) DATE

APPENDIX D

Contact Letter

Dear Participant:

My name is Judith Nyabando and I am a graduate student at East Tennessee State University. I am working in my doctorate degree in Educational Leadership and Policy Analysis. I am in the process of writing my dissertation. The name of my study is 'An Analysis of Perceived Faculty and Staff Habits that Protect or Expose them or Others to information Security Attacks.'

I would like to give a brief survey questionnaire to you. It should only take about 10 minutes to complete. You will be asked questions about your awareness of information security issues. There are no risks associated with you taking the survey.

To take the survey click on the link below:
http://www.etsu.edu/coe/UltimateSurvey/takeSurvey.asp?surveyID=64

This process is completely anonymous and confidential. In other words, there will be no way to connect your name with your responses. You will not be asked to provide any identifying information about yourself such as name and date of birth.

If you choose not to complete the survey, it will not affect you in any way.

Participation in this study is voluntary. You may refuse to participate. You can quit at any time by not submitting the survey.

If you have any research-related questions, you may contact me at (423) 433-3459 or my committee chair, Dr. Jasmine Renner at (423) 439-7629. Also the, the chairperson of the Institutional Review Board at East Tennessee State University is available at (423) 439-6055 if you have questions about your rights as a research subject. If you have any questions or you can't reach the study staff, you may call an IRB Coordinator at (423) 439-6055 or (423) 439-6002.

Sincerely

C. Judith Nyabando

VITA

CHIWARAIDZO JUDITH NYABANDO

Personal Data:	Place of Birth: Mutare, Zimbabwe
Education:	B. S., Computer Science, Bennett College, North Carolina, 2000
	M.S., Computer and Information Sciences, East Tennessee State University, Johnson City, 2003
	Ed.D., Educational Leadership and Policy Analysis, East Tennessee State University, Johnson City, 2008
Professional Experience:	Doctoral Fellow, Educational Leadership and Policy Analysis, East Tennessee State University, 2004 – 2008
	Upward Bound R.A., East Tennessee State University, Summer 2005, 2006, 2007
	Customer Service Representative, Cingular Wireless, Johnson City, Tennessee, 2003 – 2004
	Teaching Assistant, Computer and Information Sciences Department, East Tennessee State University, 2001 – 2003
	Program Assistant, 2000 – 2001, Bennett College Business Office, Greensboro, NC
	Computer Lab Assistant, 1999 – 2000
CONFERENCE PAPERS AND PRESENTATIONS:	Lampley, J. & Nyabando C. J. (2005). ELPA Technology Survey. Presented at ELPA Faculty meeting. Johnson City, TN.
	Lampley, J. & Nyabando C. J. (2006, November). Grading and attendance in doctoral programs. Paper presented at Mid-South Educational Research Association 2006 Meeting. Birmingham, AL.
	Naholi, G., Nyabando, C. J., Roach, E. & Williams, V. (2006, October). Cross cultural communication: The art of listening. Presented at College Reading and Learning Association. Austin, TX.
	Nyabando, C.J. & Lampley, J.H. (2005) *A study of Educational Leadership and Policy Analysis Doctoral Students at ETSU*. Unpublished manuscript.