5-2006

Higher Ed and Cyber Security: A Content Analysis of Two Institutions Computer Policies

Douglas P. Osowski

HIGHER ED AND CYBER SECURITY: A CONTENT ANALYSIS OF TWO INSTITUTIONS' COMPUTER POLICIES

by

Douglas P. Osowski
Candidate for Master of Science
Department of Industrial Technology
College of Business and Public Administration
University of North Dakota

An Independent Study

Submitted to Dr. Lynda Kenney, Advisor

University of North Dakota

Grand Forks, North Dakota
May
2006

This Independent Study, submitted by Douglas P. Osowski in partial fulfillment of the requirements for the Degree of Master of Science from the University of North Dakota, has been read by the Faculty Advisor under whom the work has been done and is hereby approved.

Lynda Kenney

Advisor

PERMISSION

Title	Higher Ed and Cyber Security: A Content Analysis of Two Institutions' Computer Policies
Department	Industrial Technology
Degree	Master of Science

In presenting this Independent Study in partial fulfillment of the requirements for a graduate degree from the University of North Dakota, I agree that the library of this University shall make it freely available for inspection. I further agree that permission for extensive copying for scholarly purposes may be granted by the professor who supervised my Independent Study work or, in her absence, by the chairperson of the department or the dean of the Graduate School. It is understood that any copying or publication or other use of this Independent Study or part thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the University of North Dakota in any scholarly use which may be made of any material in my Independent Study.

Signature________________________

Date May 3, 2006

ACKNOWLEDGEMENTS

First and foremost, I would like to express my sincere gratitude to my advisor Dr. Lynda Kenney for all of her valuable guidance, friendship and support with the planning and writing of this independent study. She has been patient with me and has helped with keeping this study focused and on track.

I would like to thank Therese Warmus. Therese is a family friend and she is proficient in the English language. Thank you for your input and editing skills. This was a big help and made this a more enjoyable experience.

Last but not least, I would like to thank my family for their love and support. Connie, who's patience I have tested time and time again when there were deadlines looming, has always been supportive and understanding. Thanks to my two sons, Brian and Jordan, who have always been there for help and support. Thank you to my mom who would always ask me how my studies were going and give me encouragement.

ABSTRACT

Computers and the Internet offer great benefits to society. However they can also present opportunities for crime. Breaching computer security can be summarized as committing traditional crimes using new technology tools.

The Internet and email are powerful information tools. For many colleges and universities this technology has become the preferred means of communication for staff and students. By its very nature the Internet facilitates almost instant exchange and dissemination of data, images and materials of all types. This includes not only educational and informative material but also information that might be undesirable or anti-social.

In this paper, the focus of study is the current computer security policies of two Higher Education institutions: the University of North Dakota in Grand Forks and the University of Missouri in Kansas City. The intent was to compare these policies to identify similarities and differences, and any weaknesses in cyber security. An explanation of the method of analysis is included. It was followed by an explanation of the procedures including data collection, the coding process and the importance of the limitations found by doing a comparison on these computer security policies.

Data from the two institutions were gathered and the computer security policies analyzed. This data was examined and compared in order to understand the information that the policies were written to represent.

similarities and differences. This study was qualitative in nature; the specific goal was to gather information to help determine improvements in computer security policy implementation from two universities.

The conclusion of this study showed the importance of implementing policies for educational institutions and computer user expectations. This study's primary limitation is that it does not encompass a larger pool of subjects to study. In addition, the institutions are rewriting policies as an ongoing process. During the course of the study, communication with institutional policy writers indicated more new policies were on the way.

The recommendations include: clear and concise language in policy creation, further development of unauthorized use policy, specific student use policies, high profile publication of policies, use of peer to peer software sharing, effective appeals processes, ongoing risk assessment, the need for a Computer Emergency Response Team (CERT), incidence tracking, reporting misuse and a policy for research domain names. These recommendations are offered in order to put needed policies into place for technology to be utilized to the fullest to help protect against computer security vulnerabilities.

CHAPTER I

INTRODUCTION

Computers and the Internet offer great benefits to society. However, they also present opportunities for crime. Educational institutions need to establish acceptable use policies and delineate appropriate and inappropriate actions to both students and staff (Fitzer, 2002).

The breach of computer security can be summarized as the commission of a traditional crime using new technology tools to unlawfully gain access to computers. Most schools now use technology for organizing and accessing information. Networked computers have significantly improved the speed with which administrative functions can be performed. Additionally, information regarding students, staff, courses, programs, and facilities is made much more readily available (Fitzer, 2002).

The Internet and e-mail are powerful information tools. For many colleges and universities this technology has become the preferred means of communication for staff and students. By their very nature the Internet and e-mail facilitate almost instant exchange and dissemination of data, images and materials of all types. Academic records must be secured and sensitive information must be restricted in its availability. Each institution is ultimately responsible for the integrity and security of its data; schools that fail to exercise due care and reasonable safeguards open themselves up to allegations of incompetence, negligence, law suits, and forfeiture of insurance claims (Fitzer, 2002).

Statement of Purpose

The general aim of this study is to analyze the computer security policies of two benchmark universities to determine similarities and differences. The specific goal is to gather information that will help determine improvements in computer security policy implementation.

Definitions

Computer security policies are complicated topics in their own right. Each topic has a variety of terms that can be used in a multitude of ways. A dictionary of terms is provided for the purpose of research.

Cyber is a term that refers to computers and/or computerized items both real and imagined. (Van Trieste, 2001).

Cybersecurity is the protection of data and systems in networks that are connected to the Internet (Davis, 2005).

Cybercrime is a high technological crime defined as using a computer and the internet to steal a person's identity, sell contraband, stalk victims or disrupt operations with malevolent programs (WordNet, 2003).

Hacker is the common term for those who subvert computer security without authorization (Wikipedia, 2005). *Hacking* is the act of the "hacker" taking control of a remote computer through a network, or software cracking (Wikipedia, 2005).

Cyberstalking refers to the use of the Internet, e-mail, or other electronic communication devices to stalk another person. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at an individual's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing another's property (Attorney General, 1999).

Justification of Study

Computers, their hardware, software, and interconnectivity are a significant part of our world. As this aspect of industry grows, the importance of computers and their uses increases as does the misuses of this technology.

In order to combat the increase of cyber crime, security measures are needed to protect personal and academic data gathered and generated by universities. This study will analyze two similar universities and what they are doing to combat cyber crime and to maintain their security. This study may also discover areas neglected by these two universities that can be improved to protect their data and information.

The Role of Policies in Higher Education

A policy is a plan of action for tackling political issues. It is often initiated by a political party in government, which undergoes reforms and changes by interested groups or parties. Policy designates a process. This process includes the elaboration of programs by different groups.

The University of North Dakota and the University of Missouri at Kansas City

According to Peter Johnson, Associate Director of Media Relations at the University of North Dakota (UND), the North Dakota State Board of Higher Education, with the assistance of the National Center for Higher Education Management Systems (NCHEMS), identified benchmark institutions for each of its colleges and universities. UND's list includes the University of Nevada-Reno; West Virginia University; University of Louisville; University of South Carolina at Columbia; Wright State University at

Dayton, Ohio; Southern Illinois University-Carbondale; University of Missouri at Kansas City (UMKC); Ohio University; and the State University of New York at Buffalo.

The Comparison Group Selection Service (CGSS) is designed to aid institutions in selecting a group of institutions which are similar in mission to be used in comparative data analyses. CGSS has been in use at NCHEMS since 1982 and has been used by hundreds of institutions (National, 2006).

CGSS consists of two primary components. The first is a large database containing indicator variables on each of more than 3,500 higher education institutions. This database is constructed from data files derived from the various surveys which make up the IPEDS (Integrated Postsecondary Education Data System) survey system administered by the National Center for Education Statistics (NCES, a part of the U.S. Department of Education in Washington, D.C.) (National, 2006). The indicator database contains variables covering institutional characteristics, faculty, finance, degrees awarded, enrollments, and other miscellaneous factors.

The second component of the CGSS is a set of software programs designed to condense the 3,500+ institutions in the indicator database down to a manageable list for a particular institution. This software uses a set of criteria (see discussion below) supplied by the target institution to determine which institutions appear on the possible comparison institution list and their relative rankings within the list. The CGSS yields a list of possible comparison institutions. It is the responsibility of the target institution to choose the final list of 10 to 20 institutions to become the actual comparison group.

Computer Policy Strategies

Higher education employs as many aspects of technology as audiences that utilize them. Therefore the goal of many universities is to provide top-of-the-line technologies and related services to all users. Students are a primary focus at any university and are the largest group of technology abusers that the university faces. Therefore many technological policies are geared for this group.

Specific policies have been written for the protection of students as well as that of faculty and staff. However these strategies do is not eliminate the need for specific policies protecting information pertinent to day-to-day operations of the university in addition to the irreplaceable research data being created through various departments.

Guiding Research Questions

The main research question for this study was: What policies are in place by two peer higher education institutions to meet the challenges of cyber security and to prevent cyber crimes? This question was qualitative in nature due to the need for analytical reasoning in determining the similarities and differences between the institutions' computer security policies.

Benefits of Research

It was the intent of this study to generate insight into how the computer systems of two higher education institutions are protecting their electronic information. Analysis of similarities and differences will benefit these and other universities in creating and/or amending security measures for their computer systems.

This research further intended to aid the University of North Dakota in deciding upon which security policies work best to help protect the University in its everyday operations. By conducting a comparison the author sought to determine the weaknesses that exist and to alleviate these by suggesting policy changes that fit university practices. In particular the adjustment of security policies will save time and money by cutting down the hours it takes to fix problems caused by compromised computers or servers lacking appropriate polices and procedures for security.

Universities will always be ridden with policies. Although higher education is a process designed to promote individualism and free thinking, effective policies are needed to protect students, faculty and staff without hindering the creative process. Repercussions from the lack of protection can produce negligence, inhibit forfeiture insurance claims and encourage lawsuits.

This study identified the policies from the two similar higher educational institutions. It then determined similarities and differences in the polices that each institution implemented, thereby protecting both the users and sensitive information, such as research data and academic records, in order to aid the development of enhanced security policies for the University of North Dakota.

CHAPTER II

LITERATURE REVIEW

Introduction

Higher education is the leading force in the field of research and information gathering, handling additionally the private medical and personal information of students. Computer security is imperative for privacy and accuracy.

In a recent article, Straub and Nance ascertained that 41% of computer abuse incidents were discovered by accident, 50% were discovered by systems controls and only 16% were discovered by active detection (Bouffard, 1998). With this in mind, the security of computer information in today's society is an important part of information privacy.

An overview of other studies regarding computer security is necessary to the implementation of computer policies. This ensures a variety of opinions regarding security issues that are not only obvious to a particular situation but also to what other institutions are facing in terms of security threats. The intention of the literature review is to provide a means for finding areas in need of policy implementation.

According to a study conducted by Eisler (2003), higher education policies, the rapid growth of information technology (IT), and communication networks has created wonderful opportunities for genuine growth in higher education. Linked with these opportunities are significant policy challenges that have multiple implications for access, growth, and innovation. In this rapidly evolving environment, it is critical that higher education institutions develop clear policies for access, content, acceptable and responsible use, privacy, and security for computing technology and network usage. The development of Web-based instruction has created significant new issues in the ownership and copyright of distance-learning materials. With the increase of college e-business efforts, questions surface regarding regulatory issues, financial transactions, security controls, and privacy (Eisler, 2003)

Nearly all campus employees and students now require access to a computer and computer networks. Colleges and universities have become dependent on technology for daily essential operations in administration (Eisler, 2003).

Universities are becoming increasingly dependent on fragile technologies, and may have users with limited understanding of the potential impact of their activities, and regularly face potentially destructive forces searching to exploit system weaknesses and vulnerabilities. Given an environment in which legal standards may be ambiguous and usage is increasing rapidly, responsible higher education institutions need to develop and implement policies that establish clear guidelines for university faculty, students, and staff (Eisler, 2003).

Loch, Carr and Warkentin (1992) reveal in their research that many security breaches are caused by user carelessness or maliciousness. Colleges and universities have found that students are often involved in security incidents, accidental or otherwise. To minimize attacks, administrators say, campus policies can be as important as digital security measures (McCollum, 1998).

A 1998 University of Michigan study estimated that 30 known security-related IT incidents cost over $1 million in direct and indirect costs, and resulted in the expenditure of over 9,000 employee hours for incident investigation and resolution. Nearly 270,000 computer and network users were affected. Since the study was completed, the number and complexity of cyber attacks on computer networks has increased, as have the costs of dealing with them. Managing the risks and the liabilities associated with IT-related incidents is a real and escalating challenge for higher education (Oblinger, 2004).

Many institutions do not have clear policies defining and prohibiting computer crimes. By making it clear that computer attacks are serious offenses with serious consequences, he says, administrators can discourage students who might otherwise try to see what they can get away with (McCollum, 1998).

According to Bruhn (2003), planning for IT security can be the result of a grassroots effort within the central IT organization, it can be an element of an IT strategic plan, or it can be integrated into an institution-wide strategic planning effort. There is no one "right" approach for crafting a successful IT security strategy. Each institution must evaluate its own unique interests, resources, and political climate (Bruhn, 2003).

Policy development efforts should begin with existing university policies including the student code, which serves as a contract between the student and the university (Eisler, 2003). Standards for applications development, systems development and controls need to be defined and implemented early in the computer systems development. The standards define certain basic efforts that must be taken to assure a minimum level of quality, security and legal compliance (Bouffard, 1998).

There is tremendous diversity in the type and quality of hardware and software utilized across an institution, ranging from outdated to state-of-the-art. The variety of equipment ownership—from student-owned computers to federally funded supercomputers—is also a complicating factor. The student population is transient and comes to campus with no real appreciation of security issues (Bruhn, 2003).

System Security includes all system-wide, application independent software and hardware based security methods, including network security. These issues include: a network firewall to protect organizational data from external threats, remote terminal physical security (Parker, 1982), restriction of systems utility programs (Parker, 1982), data classification (Parker, 1982; Ruder and Madden, 1978), technical reviews of operating system changes (Parker, 1982; Ruder and Madden, 1978), user authentication (Parker, 1982; Ruder and Madden, 1978), automatic, timed, terminal logoff (Ruder and Madden, 1978).

A user agreement stipulates the rules and regulations that must be followed for proper and secure use of the system (Bouffard, 1998). Users should be encouraged to report suspected security breaches. They should also learn to appreciate that illegal access or sabotage could effect user performance and productivity as well as damage the organization as a whole (Wong, 1987).

Information-collection practices across the institution need to be inventoried. Fair information practices (including the principles of notification; minimization; secondary use; nondisclosure and consent; need to know; data accuracy; inspection and review; information security, integrity, and accountability; and education) should be established and promoted. A privacy statement should inform all individuals from whom information is collected of the institution's privacy policies and practices (Petersen, 2005).

Ideally, the question of whether or not to notify will have been previously rehearsed and dictated as part of an overall incident-response plan. The establishmer policies, procedures, and protocols for the handling of data security incidents will pay o when crisis mode sets in. However, once the policies and procedures are established, they need to be followed, lest the institution create an additional source of liability (Petersen, 2005).

Communication and information systems in higher education processes, communication, scholarship, research, and learning are technologies that must be both reliable and secure. With increased numbers of users and near exponential increases in use, campuses need policies and guidelines that set forth clear expectations and standards for use (Eisler, 2003).

Wada and King (2001) suggest that there are lessons in the formation of effective IT policy, noting that technology is evolving much more quickly than law and business practices and that answers to accompanying policy questions develop more slowly. This vironment requires both new policy and constant interpretation of existing policy. As a IT staff can be placed in the position where they must decide what is appropriate Eisler, 2003).

llege and university information technology staff and functional offices are r the development of an institutional "information security policy." A place would be a statement of strategic direction that identifies chnology security as a priority and assigns appropriate authority to program (Bruhn, 2003).

One thing is clear: Network security is everyone's responsibility. While it would be more convenient if the solution were a piece of technology, and it's tempting to rely on IT staff or information security officers to ensure cyber security, the problem is more complex. It will take a coordinated effort to develop an effective cyber security program. It is an ongoing challenge that requires the cooperation and vigilance of administrators, faculty, staff, and students, and the leadership and cooperation of senior executives, legal counsel, auditors, police and public safety, and others. A successful academic security strategy involves technology, policy, and people (Oblinger, 2004).

Higher Education’s Role in Policy Development

Research conducted by Oblinger (2004) discovered that bad things can happen in cyberspace. The free and unimpeded flow of information and ideas now relies directly upon adequate security because breaches, hacker attacks, and viruses can quickly take down the networks upon which research, instruction, and communication depend. Information security is an increasingly important responsibility for all organizations--particularly academic institutions. But just how large a problem do security incidents (which can range from unauthorized access, alteration of data, and virus infiltrations, to denial-of-service attacks) actually present to Institutions of Higher Education (IHEs)?

Forces include any threats to the organization. These include, but are not limited to: viruses, hackers, fire and other disasters, employee accident and malicious actions, power failures etc. The list of threats to any organization is extensive and cannot be generalized. Each organization has threats particular to it based on competition, geographic location, past history, size and other factors (Bouffard, 1998).

Some segments of the higher education community continue to believe that security and academic freedom are antithetical. Academic environments are characterized as communities of tolerance and experimentation, where anonymity is highly valued (Bruhn, 2003). Proactive security measures may be viewed as too "bureaucratic" by faculty, deans, researchers, and others in the academic arena (Bruhn, 2003).

The responsibility of higher education to cyber security goes beyond keeping its slice of cyberspace safe. Higher Ed can play a larger leadership role for government and industry by providing guidance and innovation in digital security issues (Oblinger, 2004). For higher education, the key factor for success in the security effort will be the ongoing development and refinement of effective security strategies and plans (Bruhn, 2003). Electronic data issues go beyond relationships between the university, faculty or staff member, and student to include data exchange between education providers (Eisler, 2003). With increase transfer of credits and the growth of lifelong learning, electronic interactivity among universities is important for the future of higher education (Eisler, 2003).

Part of the educational responsibility for colleges and universities is to educate people in appropriate cyber behavior. Policies regarding acceptable and responsible use cover a variety of other user functions and expectations (Bruhn, 2003). Studies show a need for continued proactive collaboration among United States higher education institutions if they are to remain information technology policy leaders. It looks to the crisis brought about by computer hacking and denial-of-service attacks' on web sites and media scrutiny received by colleges and universities, mainly for their close relationships with federal research (Sern, 2000).

University computing facilities are for educational and university purposes; it is inappropriate to use these university resources for commercial or political purposes. In comparison with policies in industry, universities tend to be more lenient concerning computer use for personal reasons (Eisler, 2003). For higher education, the key factor for success in the security effort will be the ongoing development and refinement of effective security strategies and plans (Bruhn, 2003).

Hackers/Unauthorized Users Access

According to Wikipedia (2005), hacker is the common term for those individuals who subvert computer security without authorization. Hacking is the act of the "hacker" taking control of a remote computer through a network, or software cracking (Wikipedia, 2005).

Consensus among network administrators is that the majority of hacking incidents affecting universities are the work of novices. They are denial-of-service attacks that disable individual computers and whole campus networks. Because data is tempting to serious hackers, policies need to be implemented to minimize attacks (McCollum, 1998).

With computer hacking on the rise, colleges seek ways to handle attacks. Campus systems face both malicious incidents and pranks that escalate unintentionally. Malicious hackers have crashed hundreds of PCs in university computing labs, drowned campus networks in worthless data, and coated college Web pages with digital graffiti. It's enough to make an institution consider unplugging its network (McCollum, 1998).

But saner heads have prevailed. The consensus among network administrators seems to be that while skilled hackers might try to crack campus networks once in a while, most hacking incidents that affect colleges and universities are the work of novices who don't realize how much damage their electronic mischief can cause. Still, experts say, administrators are asking for trouble if they don't keep a close eye on their networks and make some basic technical and administrative preparations for dealing with hackers (McCollum, 1998).

During the first week of March 1998, computer users on at least 25 campuses and at several government research laboratories saw scores of their desktop computers crash, almost in unison. An as-yet-unidentified attacker, or perhaps a group of attackers, had exploited a weakness in the Windows 95 and Windows NT operating systems to crash thousands of machines nationwide by overloading them with digital information. Such invasions are known as denial-of-service attacks, and while they may not cause permanent damage or compromise private information, they can make individual computers or whole campus networks temporarily unusable (McCollum, 1998).

The Harvey Mudd network is configured to prevent people on the campus from using Internet Protocol (IP) spoofing, with which an attacker can disguise his or her computer with the address of another machine, even one on another network or another campus. A disguised address would help a hacker launch some attacks more easily—and more anonymously (McCollum, 1998).

Application security is necessary to assure that source code and data files can be modified only by authorized users and that these changes will conform to security standards. This is a critical function and along with it goes the added burden of regulating authorized users' access to applications and data files (Thuraisingham and Rubinovitz, 1992; Thuraisingham 1992; McHugh and Thuraisingham, 1988).

"Sniffer" techniques used by crackers—malevolent computer hackers—to gather passwords can easily be adapted to allow surreptitious monitoring of electronic-mail messages and other types of data that move along the Internet. In fact, the techniques can be used on virtually any computer that is connected to any kind of network (Wilson, 1994).

A firewall is a set of hardware and software used to protect one network from another un-trusted network. The typical firewall can be thought of as a pair of mechanisms: one which exists to block traffic and the other which exists to permit traffic. Emphasis can be placed on either of these functions (Ranum, 1994).

A formal procedure must be undertaken by any users wishing to gain access, or change their current access, to the computer (Bouffard, 1998). The purpose of this method is to restrict access to terminals to authorized users (Bouffard, 1998). Another such method is requiring all terminals to be located within a secure perimeter to minimize potential misuse. Automatic terminal timed shutoff should be implemented to restrict unauthorized access to an unoccupied and forgotten terminal (Bouffard, 1998).

In February 2000, near the start of the "new millennium," many unsecured college and university computers, among others, were used by hackers on the Internet to launch "denial-of-service" attacks on popular commercial Web sites. Even though campus computers represented only a fraction of those used in the attacks, colleges and universities received much media scrutiny, mainly for their high profiles and their close relationships with federal research (Sern, 2000).

Colleges and universities are trying to teach their faculty and students to be responsible network users—users who are aware that their individual actions can affect the entire networked community (Sern, 2000). Access policies establish rights for users as well as expectations on how those resources will be used. Access normally extends to all members of the university community and may also be provided to prospective students and alumni. Approaches are designed so that users can access information they are permitted to see, but no more than this, and to change information they can change and no more. Users have the basic rights of a fair share of resources. These rights are not transferable to others (Eisler, 2003).

Your electronic-mail account maybe telling people a lot more than you can imagine. With a tool called "Finger," users connected to the Internet anywhere in the world can frequently find out your electronic-mail address, your name, whether you're working on your computer, how long it's been since you last checked you mail, who has sent you mail, and event the exact location from which you are logging in (Wilson, 1994). The use of the tool has touched off a widespread debate between those who see Finger as the equivalent of directory assistance for the Internet and those who say its hazards out weigh its benefits (Wilson, 1994).

Many college and university computer-system administrators have responded to concerns about Finger by restricting it. Some administrators have modified the tool so that it doesn't give out information considered sensitive. Others, without the expertise or the resources to tinker with the structure of the software underlying Finger, have removed it from their systems entirely (Wilson, 1994). Most administrators say they have restricted Finger because they are afraid that crackers can use it to obtain information that enables them to break into computer accounts and create mischief (Wilson, 1994).

Cybersecurity is the protection of data and systems in networks that are connected to the Internet (Davis, 2005). In today's distributed environment, it is not uncommon for a user to download some data for local processing or analysis. Once this data leaves the confines of the corporate database there is no guarantee of protection; the security aspect of distributed databases is currently a very hot issue (Thuraisinghamand Rubinovitz, 1992; Thuraisingham, 1991; Goyal and Singh, 1991; Laferriere, 1990; McHugh and Thuraisingham, 1988). Corporate data is the lifeblood of the organization, and making it tamper-proof should be of the highest concern (Parker, 1982). This can be a very difficult task and since the data on a computer system is often its most valuable resource (Wong, 1987), a critical one. The saying that "information is power" was born upon this realization. Data security methods include: production program authorized version validation (Parker, 1982), program quality assurance (Parker, 1982; Ruder and Madden, 1978), program change logs (Parker, 1982), secrecy of data file and application names (Parker, 1982), data file access controls by sub-function (Parker, 1982), application program testing policy (Ruber and Madden, 1978), initial program load (IPL) checks (Ruder and Madden, 1978), processing time controls (Ruder and Madden, 1978) (Bouffard, 1998).

Content is one of the thornier issues for university technology policies. Academic freedom is a tenet of higher education and carries with it expectations for unrestricted access to Internet materials. Although institutions may reserve the right to restrict access, university policies rarely include instances of Internet filtering. One notable exception was the decision by universities during the 2000–01 academic year to restrict access to Napster. Some campuses took this action because of bandwidth concerns or to avoid copyright infringement (Eisler, 2003).

College networks may offer little that is of monetary value for hackers but there are nevertheless prizes that a serious attacker might be eager to steal, says Eugene H. Spafford, computer-science professor at Purdue University and director of its research program in computer security. Intellectual property, such as scientific data and academic-research results, could attract hackers as could licensed copies of expensive software packages. Some institutions, he adds, may keep information such as credit-card and Social Security numbers on their networks as part of on-line registration systems. But, it's "relatively rare" for attackers to go after such information, Spafford reports. Most security experts suggest that any data worth stealing be kept on computers that are not accessible via the Internet (McCollum, 1998).

"If scientists cannot be certain that their research data will not be altered, if patients do not trust the privacy of their medical records, and if the safety of financial information is in doubt, then the value of the Internet will be sharply curtailed," said Rep. Rick Boucher, Democrat of Virginia and chairman of the subcommittee. "Threats to Internet security will reverberate far beyond the Internet's current boundaries" (Wilson, 1994).

Flaming and Cyberstalking

As in other forms of communication, computer users need to follow university standards regarding discrimination and harassment. The immediacy of computer technology such as e-mail, instant messaging, and discussion postings can encourage users to respond in the emotion of the moment, without reflection. Working at a computer can create a feeling of impersonality in which users may send thoughtless and tasteless items. When this impersonal communication is carried to the extreme correspondence can be considered *flaming*, the sending of a message that may be openly hostile, rude, bigoted, sexist, or obscene (Eisler, 2003). The government has developed clear federal guidelines and expectations for universities to deal with student data and personal information. With the exception of the financial aid process, most campuses have replaced the use of Social Security numbers with randomly generated student identification numbers accompanied by a personal identification number. Unlike commercial entities, higher education institutions rarely track or monitor Internet usage or electronic correspondence. Policies preserve the right of colleges and universities to do so on occasion when dealing with complaints or reports of abuse. It is the normal expectation that electronic files will be treated as personal and confidential. Enforcement of more rigid policies, except in cases of clear abuse, can be difficult (Eisler, 2003).

Cyberstalking is the term used in this report to refer to the use of the Internet, e-mail or other electronic communications devices to stalk another person. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects or vandalizing a person's property (Attorney General, 1999).

While some conduct involving annoying or menacing behavior might fall short of illegal stalking, such behavior may be a prelude to stalking and violence and should be treated seriously (Attorney General, 1999).

policies. When possible, they should reference and draw from extant policies rather than create duplicate standards for information (Eisler, 2003). The goal is to be clear and intelligible when explaining appropriate and inappropriate activities and behaviors. Policies should reference explanations of due process rights and possible sanctions for violators. Additionally, policies should be available and easily accessible for users. Some institutions include the completion of user education as a requirement for network access (Eisler, 2003).

It is important to compare the findings from this study against the results of similar studies to develop a solid frame work, setting up a benchmark for evaluating results and making the best recommendations. Because of the rapidly changing environment of technology, ongoing study of security policy issues must remain constant. New technologies mean new ways to compromise computers, invading personal lives and disrupting information processes; the development of new means to combat such invasions is imperative.

CHAPTER III

METHODOLOGY

This study was designed to compare the computer security policies between the University of North Dakota and University of Missouri at Kansas City. As the realm of technology grows, so does the need to protect the individuals and the institutions using it. Upon the request of a former Chief Information Officer (CIO) at the University of North Dakota on technology security issues for the campus, this study was implemented to analyze the policies of two similar higher education institutions regarding computer security to fend off cyber crime. The specific intent and design of this study focused on the policies regarding computer use at two higher education institutions of similar size and student composition. The two schools chosen for the study were considered peer universities identified by the North Dakota State Board of Higher Education and the National Center for Higher Education Management Systems.

This chapter includes an explanation of the method of analysis that was used. It is followed by an explanation of the procedures, including data collection and the coding process of the computer security policies.

Qualitative Method of Content Analysis

In this study, the chosen research method is a content analysis. A content analysis is a detailed and systematic examination of the contents of a particular body of material for the purpose of identifying patterns, themes, or biases. Content analyses are typically performed on forms of human communication, including books, newspapers films, television, art, music, and videotapes of human interaction and transcripts of conversations (Leedy, 2001).

Content analysis is a research tool used to determine the presence of certain words or concepts within texts or sets of texts. Researchers quantify and analyze the presence, meanings and relationships of such words and concepts, then make inferences about the messages within the texts, the writer(s), the audience, and even the culture and time of which these are a part. Texts can be defined broadly as books, book chapters, essays, interviews, discussions, newspaper headlines and articles, historical documents, speeches, conversations, advertising, theater, informal conversation, or any other occurrence of communicative language. (Busch, 2005).

To conduct a content analysis on any such text, the text is coded or broken down into manageable categories on a variety of levels—word, word sense, phrase, sentence, or theme—and then examined using one of content analysis' basic methods: conceptual analysis or relational analysis. (Busch, 2005).

The research for this study was conducted by inquiring the usefulness of security policies and addressing issues about their usability and accuracy. A content analysis was employed to observe the areas of focus and classifications pertaining to the policies that are a good fit for the University of North Dakota. This method helped focus, without bias, on the content by isolating the vocabulary, allowing their essential implication to become understandable.

Procedure

The procedure for this study began with a literature review that uncovered computer security areas that could be dangerous to an individual's welfare as well as to institutional data protection. Computer security policies were constructed to address these relevant issues. A study on these computer policies was necessary to recognize gaps determining whether or not policies address pertinent computer security issues.

Data Collection

According to Peter Johnson, Associate Director of Media Relations at UND, the North Dakota State Board of Higher Education, with the assistance of the National Center for Higher Education Management Systems, benchmark institutions were identified for each of its colleges and universities. UND's list included the University of Nevada-Reno, West Virginia University, University of Louisville, University of South Carolina at Columbia, Wright State University Dayton, Ohio, Southern Illinois University-Carbondale, University of Missouri at Kansas City, Ohio University, and the State University of New York at Buffalo. UND was chosen because its former CIO requested the study be completed. UMKC was chosen because they were one of UND's peer universities that responded to the request to participate in the study.

After contacting the chief information officers at UND and UMKC, and obtaining their agreement to cooperate with this study, gathering the data from the Internet was the next step (see Appendices A, B). The data was gathered via the Internet web page for each institution. This information consisted of policies that these institutions used to identify procedures they wanted computer users to follow.

After data was collected, analysis began. As a general rule, a content analysis is quite systematic and measures are taken to make the process as objective as possible. Both institutions' policies were easily obtainable from the Internet. The lack of current information on a university's Web site forms the only limitation to this type of information gathering.

Coding Process

The coding process for this study consisted of reading all of the policies and breaking down the text into lists of words and then phrases if possible. The coding entailed separating the word phrases into two categories: similarities and differences.

The headings for UND policies consisted of Definitions, Individual Privileges, Individual Responsibilities, Institution Privileges, Institution Responsibilities and Procedures and Sanctions. The headings for UMKC policies consisted of Acceptable Use, Unacceptable Use, Enforcement of Policy, Non-Commercial Use Explanation, Security Service Policy, Security Team, Team Coordination, Security Incident Response, Acceptable Use Policy Incident Response and Security Practices.

It was evident that these policies were not consistent in their heading listings, constituting differences. It was discovered that faster results were gained by copying and pasting the policies into Microsoft Word software then conducting searches to look for similarities and differences in content.

During this process, patterns emerged. For instance, there were policies regarding hacking, security data, and harassment; they were coded as "hacking", "security data" and "harassment". As the analysis progressed the number of categories or topics grew.

After examination of the word lists was completed, analysis of the computer security policies between the two universities began.

Summary

This chapter explained the methods used for conducting the comparison on the computer security policies. This consisted of performing a content analysis on the security policies between the University of North Dakota and the University of Missouri at Kansas City. A study on these computer policies was necessary to recognize similarities and differences determining whether or not the policies address pertinent computer security issues. The next chapter will analyze the security policies gathered from UND and UMKC. This information will then be examined through content analysis and comparison of the two universities policies.

CHAPTER IV

DATA

The purpose of this chapter is to analyze the security policies gathered from the University of North Dakota and University of Missouri at Kansas City. This information will then be scrutinized and compared for differences and similarities.

Both the University of North Dakota and the University of Missouri at Kansas City serve their communities of faculty, administration, staff and students with state-of-the-art technological advances. In order to be able to adequately support each separate entity within the university, a system of authority has been put in place to create policies regarding these technologies.

UND must follow the policy guidelines of the North Dakota University System (NDUS). NDUS incorporates 11 public colleges and universities across the State of North Dakota and is governed by the State Board of Higher Education. Organized as a system in 1990, NDUS includes two doctoral universities, two master's degree-granting universities, three universities that offer bachelor's degrees and five two-year colleges that offer associate and trade/technical degrees. NDUS has developed a comprehensive list of policies regarding computer use on campuses (NDUS, 2006).

UMKC must also follow policies pertinent to their university within the guidelines of the outside entity of Missouri Research and Education Network (MOREnet). MOREnet provides Internet connectivity, access to Internet2, technical support, videoconferencing services and training to Missouri's K-12 schools, colleges and universities, public libraries, health care, state government and other affiliated organizations (MOREnet, 2006).

Established in 1991, MOREnet operates as a unit within the University of Missouri, and is based in Columbia, Missouri. The MOREnet network is the foundation infrastructure. Members of the education community interact with each other via data and video services; public sector business applications are built and conducted on it; and Missouri citizens interact with their state government through it (MOREnet, 2006).

In addition to the set of polices NDUS and MOREnet have for their respective state universities, each university has its own individual institutional polices to cover the vast computer concerns. Individual policies are tailored to protect their universities ongoing and growing threats in a field where new technologies emerge.

The following information conveys the acceptable use policies from NDUS and MOREnet that UND and UMKC must follow regarding their computer systems security. Next the data that was found to be different and similar is reported.

Similarities

Acceptable and Unacceptable Use Policies

Each institution has policies outlining acceptable and unacceptable use for their Information Technology systems. UND does not directly headline acceptable use; it is identified throughout their written policies and the NDUS policies, and agrees with MOREnet's policy, which is easily identified. The policy can be paraphrased to say that acceptable users are project participants who are in support of research, education, local, state or national government affairs, economic development or public service (NDUS, 2006).

The acceptable use policy is not identified in the NDUS policy directly however it is identified indirectly throughout the policy. The areas that are similar to acceptable use are compliance with NDUS and institution policy, and all laws and contracts regarding the use of information that is the property of others (NDUS, 2006).

All network use by MOREnet members, project participants and those connected via MOREnet members or project participants shall be for or in support of research, education, local, state or national government affairs, economic development or public service (MOREnet, 2006).

As with the acceptable use definition policy, the unacceptable use policy discourages violations of federal or state law, the intellectual property rights of others and intentionally or negligently disrupts normal network use and service. Such disruption would include the intentional or negligent propagation of computer viruses, the violation of personal privacy, and the unauthorized access to protected and private network resources.

At both universities it is unacceptable to use technological resources for commercial activities that are not in support of education, research, public service, economic development or government purposes. This is evidently expressed in the policies of each institution.

Intellectual Property. When reproducing or distributing information, users are responsible for the observation of copyright rights and other intellectual property rights of others and all state and federal without the owner's permission. Written consent from the copyright owner is normally necessary to reproduce or distribute copyrighted material. There are some exceptions such as fair use in teaching and research (NDUS, 2006).

Users may not use NDUS or NDUS Institution computers or networks to harass any other person. Prohibited activities include, but are not limited to: (1) intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) intentionally using the computer to contact another person repeatedly with the intent to annoy, harass or bother, whether or not an actual message is communicated, and/or the purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease; (3) intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right or institutional sanction to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease; (4) intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another; or (5) intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another (NDUS, 2006).

Recognizing and honoring the intellectual property or a right of others is a good practice to follow. Users should not use, copy, store or redistribute copyrighted material or violate copyright or patent laws concerning computer software licenses or documentation. Generally, materials owned by others cannot be used without the owner's written permission. Students should also be careful of the unauthorized use of trademarks (NDUS, 2006).

It is not acceptable to use MOREnet for any purpose which violates the intellectual property rights of others (MOREnet, 2006). This is stated in MOREnet's policies clear and concise.

Viruses. Students should refrain from any and all activities that are intended to damage IT resources or compromise the integrity of the network, computer systems, or data. This includes, but is not limited to, all items in the Inappropriate Use section of this policy (NDUS, 2006).

Interference with the operation of computer systems or network is an ongoing threat. Deliberate attempts to degrade or interfere with the performance or integrity of any IT resource or to deprive authorized individuals access to any resource are prohibited. Some examples include propagating worms or viruses, denial of service attacks, or broadcasting, spamming, or mass mailing messages to large numbers of individuals (NDUS, 2006).

It is not acceptable to use MOREnet in a manner that intentionally or negligently disrupts normal network use and service. Such disruption would include the intentional or negligent propagation of computer viruses, the violation of personal privacy, and the unauthorized access to protected and private network resources (MOREnet, 2006).

Privacy Rights. Individuals are prohibited from looking at, copying, altering, or destroying another individual's electronic information with out explicit permission (unless authorized or required to do so by law or regulation) (NDUS, 2006). Users must comply with NDUS and Institution policy and all laws and contracts regarding the use of information that is the property of others. Documentation of consent to use copyrighted materials must be kept on record and made available to institution officials upon request. The NDUS assumes no obligation to monitor their customers (NDUS, 2006).

Respecting the rights and privacy of others is the responsibility of the user. Students who use the university's IT resources are expected to respect the privacy and personal rights of others. Individuals are prohibited from looking at, copying, altering or destroying another individual's electronic information without explicit permission. Students should also be respectful when using computing systems to communicate with others (NDUS, 2006).

It is not acceptable to use MOREnet in a manner that intentionally or negligently disrupts normal network use and service. Such disruption would include the intentional or negligent propagation of computer viruses, the violation of personal privacy, and the unauthorized access to protected and private network resources (MOREnet, 2006).

Business-related violations. Computing and networking resources may not be used in connection with compensated outside work or for private business purposes unrelated to the NDUS or institutions, except in accordance with the NDUS Consulting Policy. Users should also be careful of the unauthorized use of trademarks. Certain uses of such marks online on Web sites or in domain names can constitute trademark infringement. Unauthorized use of an institution's name in these situations can also constitute trademark infringement (NDUS, 2006).

Users are responsible for knowing to which resources they have been granted access. Refraining from all acts that waste or prevent others from using these resources, or from using them in ways proscribed by the NDUS or NDUS institutions or state or federal laws (NDUS, 2006).

Computing and networking resources may not be used in connection with compensated outside work or for private business purposes unrelated to the NDUS institutions except in accordance with institutional consulting policies. This issue has to be addressed if it is found (NDUS, 2006).

Unauthorized port scanning, network scanning, banner grabbing and other forms of reconnaissance are violations. While these activities are commonly viewed as reconnaissance prior to an attack, they gather only publicly visible information. Scans are security events, but not viewed as critical for triage purposes. Scanning in large volume, however, can create denial of service conditions (MOREnet, 2006).

Security/Firewalls. Anti-virus software should be installed and any software installed (especially operating system and anti-virus software) should be kept up-to-date with regard to security patches. Personal firewalls should be deployed when their installation will not interfere with the function of the device or the administration of the network; and such firewalls should be configured to allow minimal traffic (NDUS, 2006).

Users are prohibited from attempting to circumvent or subvert any system's security measures. Any security incidents should be reported to the system administrators and the Campus IT Security Officer. Authorized users may not damage computer systems, obtain extra resources not authorized to them, deprive another user of authorized resources, or gain unauthorized access to systems by using knowledge of: a special password, loopholes in computer security systems, another user's password, or access abilities used during a previous position (NDUS, 2006).

Deliberate attempts to degrade the performance of any computer system or network or to deprive authorized personnel of resources or access to any computer system or network are prohibited. Harmful activities are prohibited. Examples include, but are not limited to, Internet Protocol (IP) spoofing; creating and propagating viruses; port scanning; disrupting services; damaging files; or intentional destruction of or damage to equipment, software, or data (NDUS, 2006).

Access to computing and networking resources, computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. Users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information. Users are responsible for any use or misuse of their authentication information and authorized services (NDUS, 2006).

Use of NDUS computing facilities to commit acts of academic dishonesty will be handled through existing campus procedures which address allegations of academic dishonesty. This does happen and has to be addressed when it is identified (NDUS, 2006).

Maintaining the security of personal computers is an ongoing process left up to the user. Students are responsible for maintaining the security of their personal computers in order to ensure the integrity of the campus network. Personal firewalls should be installed configured and enabled to allow only the needed programs and services (NDUS, 2006).

According to both NDUS and MOREnet, anti-virus software should be installed and any software installed should be kept up-to-date with regard to security patches. Personal firewalls should not interfere with the function of the device or the administration of the network.

Customers are strongly encouraged to defend their own networks and to implement sound security policies, maintenance and change control practices, architecture and enabling technologies (such as firewalls) in defense of their own networks. MOREnet does not have funding or staff to maintain customer internal networks and devices (MOREnet, 2006).

Reporting misuse. All users and units have the responsibility to report any discovered, unauthorized access attempts or other improper usage of institutional computing and networking resources. Immediate steps are necessary to ensure the safety and well being of information resources (NDUS, 2006).

Penalties for infractions of policies are generally resolved informally by the unit administering the accounts or network in conjunction with the Campus Information Technology Security Officer. Subsequent and/or major violations may result in immediate loss of computer access privileges or the temporary or permanent modification of those privileges (NDUS, 2006). The following procedure is used:

1. Take immediate steps as necessary to ensure the safety and well being of information resources. For example, if warranted, a system administrator should be contacted to temporarily disable any offending or apparently compromised computer accounts, or to temporarily disconnect or block offending computers from the network (see sections 4.5, 4.6 and 4.7, NDUS, 2006).
2. First and minor infractions of these policies are generally resolved informally by the unit administering the accounts or network in conjunction with the Campus Information Technology Security Officer. Minor infractions are those in which the impact on the computer or network resource is minimal and limited to the local network. Resolution of

the infraction will include referral to the Code of Student Life, staff or faculty handbooks, or other resources for self-education about appropriate use. In the case of students, a copy of the resolution will be sent to the Campus Judicial Officer (NDUS, 2006).

3. Subsequent and/or major violations Repeated minor infractions or more serious misconduct may result in immediate loss of computer access privileges or the temporary or permanent modification of those privileges. More serious violations include, but are not limited to, unauthorized use of computing facilities, attempts to steal passwords or data, unauthorized use, distribution or copying of licensed software, or other copyrighted materials, use of another's account, harassment or threatening behavior, or crashing the system. Policy violators will be referred by the campus Information Technology Security Officer to the Campus Judicial Officer for further action (NDUS, 2006).

4. Range of disciplinary sanctions: Users who violate this policy are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary action, dismissal from the institution, and legal action. Use that is judged excessive, wasteful, or unauthorized may result in denial of access to computing and networking resources and may subject the user to appropriate disciplinary and/or legal procedures. Any offense which violates local, state, or federal laws may result in the immediate loss of all computing and networking resource privileges and will be referred to appropriate college or university offices and/or law enforcement authorities (NDUS, 2006).

5. An appeals notice of violations and appeals of decisions will follow campus procedures (NDUS, 2006).

MOREnet regularly reports summaries of security reports and resolutions to their Computer Emergency Response Team (CERT) for inclusion in CERT reports. These reports include information on all incidents, but include only specific data about the incident(s) which has been authorized for release by the customer reporting. Any reports to CERT, MOREnet committees or other external sources will not identify specific customers, nor will the reports be generated in such a manner that specific customers could be identified unless the customer specifically releases MOREnet to do so (MOREnet, 2006).

Differences

Policies Specific to NDUS

Unauthorized Use. Also discussed in the policies were unauthorized use and the protection of system access. Authorized users may not damage computer systems, obtain extra resources not authorized to them, deprive another user of authorized resources, or gain unauthorized access to systems by using knowledge of, a special password, loopholes in computer security systems, another user's password, or access abilities used during a previous position (NDUS, 2006).

Interdepartmental policies. Students must respect and follow the policies and procedures regarding the use of IT resources. It is required by the student's home college or department, when not in conflict with university or NDUS policies and procedures (NDUS, 2006).

Copyrights. Users are responsible for recognizing and honoring the intellectual property rights of others. Users are prohibited from using, inspecting, copying, storing, and redistributing copyrighted material and computer programs in violation of copyright laws. Software must be properly licensed and all users must strictly adhere to all license provisions (NDUS, 2006).

Hacking. Access to computing and networking resources, computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. Users are responsible for any use or misuse of their authentication information and authorized services.

Students must not compromise the privacy or security of information by attempting to access or acquire data on restricted portions of the network, network applications, databases or individual computer systems without appropriate authorization by the system owner or administrator. Students should not attempt to circumvent or subvert any system's security measures or data protection schemes or exploit security loopholes to gain access to systems or data (NDUS, 2006).

Use by others of personal accounts. Students are given individual user accounts and passwords to provide access to computer and networking resources. These accounts and passwords must not be shared with others. Likewise, students should never use the account or password of another individual to access a computer or network resource (NDUS, 2006).

Use of tools to assess security or attack computer systems or networks. Students must not download and/or use tools that are used to assess the security or attack computer systems or networks, or used to monitor communications (NDUS, 2006).

Harassment. Users may not use NDUS Institution computers or networks to harass any other person. Prohibited activities include, but are not limited to: (1) intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) intentionally using the computer to contact another person repeatedly with the intent to annoy, harass or bother, whether or not an actual message is communicated, and/or the purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease; (3) intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right or institutional sanction to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease; (4) intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another; or (5) intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another (NDUS, 2006).

Inappropriate Use. Students must refrain from any and all activities that are intended to damage IT resources or compromise the integrity of the network, computer systems, or data. Deliberate attempts to degrade the performance of any computer system or network or to deprive authorized personnel of resources or access to any computer system or network are prohibited (NDUS, 2006).

Wasting Resources. Users are responsible for knowing to which resources they have been granted access and refraining from all acts that waste or prevent others from using these resources. Users are prohibited from attempting to circumvent or subvert any system's security measures (NDUS, 2006).

Threats. Students are prohibited from using IT resources for the purpose of threats, violence, obscenity, slander, and child pornography and to observe copyrights, licenses, trademarks, and intellectual property rights. Student's use of IT resources must follow all university policies, regulations, procedures, and rules (NDUS, 2006).

Anonymous identity. Users must not attempt to conceal their identity when using IT resources, except when the option of anonymous access is explicitly authorized. False identities are strictly prohibited (NDUS, 2006).

Damaged resources. Attempting to alter an IT resource or attempt to alter the hardware or software configuration without the explicit permission from the system or network owner or administrator is prohibited. This is a necessary procedure to keep the network up and running (NDUS, 2006).

Consequences/Appeals. Academic dishonesty will be handled through existing campus procedures which address allegations of academic dishonesty. Students who violate this policy will be subject to sanctions administered by the appropriate college, department, system owner, or network owner. This may include warnings, immediate loss of network or system access privileges or the temporary or permanent modification of those privileges.

Repeated or severe violations of this policy will result in the student being referred to the Dean of Students Office to administer disciplinary sanctions as outlined in Section 2-4 of the Code of Student Life. The basic sanctions are "Written Reprimand", "Warning Probation", "Conduct Probation", "Suspension", and "Indefinite Suspension".

Any offense which violates local, state, or federal laws may result in the immediate loss of all computing and networking resource privileges. This will be referred to appropriate law enforcement authorities (NDUS, 2006).

appeals process

violators referred to the Dead of

followed as outlined in Section 2-8 of the Code of

Individuals who use University of North Dakota computer la

responsibility of seeing that these resources are used in the appropriate manner. Misu

computer facilities is considered a violation of University policy and regulations and may also be a violation of law if data of other computer users are disturbed or the privacy rights of individuals are violated. Prohibited activities include, but are not limited to, the following:

1. Chain Letters: A letter sent to several persons with a request that each send copies of the letter to an equal number of persons.

2. Spamming: Internet equivalent of junk mail.

3. E-mail Bombing: Sending repeat messages to other persons many times over to clog their mail boxes and to cause them to waste their time deleting those messages.

4. Mail Spoofing: Sending mail so as to appear to come from someone other than the actual sender.

5. Ping Flooding: Shutting down an Internet user or provider by jamming the communication channels.

6. Packet Sniffing: Putting a network interface card in the promiscuous mode in order to see data destined for other machines.

7. Password Cracking: Using applications such as crack or crackerjack to do password guessing of servers.

However the security officer on UND's campus has designated a team for incident response. This team investigates any incident that is threatening to the University computer network system. Although there is no formal incident response policy or procedure in place, there is an informal incident response procedure that exists to identify incidents and responds through a Computer Emergency Response Team (CERT). The IT Security Officer for the campus is currently setting up an incident response team. Doing this will abolish inconsistencies and recognize the various roles in the incident response development.

MOREnet cooperates with the Computer Emergency Response Team located at the university for reporting and resolution of security incidents. The CERT Coordination Center is the organization that grew from the computer emergency response to the needs identified during the "Internet Worm" incident, a malicious program that shut down about 6,000 government and university computers. The CERT charter is intended to work with the Internet community to facilitate its response to computer security events involving Internet hosts; to take proactive steps to raise the community's awareness of computer security issues; and to conduct research targeted at improving the security of existing systems. Currently, UND and NDUS policies do not address technology training.

Policies Specific to MOREnet

Defining Commercial Activities. Due to its broader application in the community, MOREnet places exacting restrictions upon student use concerning commercial activity not addressed in NDUS policy. Commercial activity means that students may not sell connections, advertise commercial products using a MOREnet connection or MOREnet provided/managed server, sell products or services directly through using a MOREnet connection or MOREnet provided/managed server, or provide electronic mail accounts for the furtherance of commercial activities as noted above (MOREnet, 2006).

Examples for MOREnet to follow. The following lists of permissible and prohibited activities are not exhaustive, but merely represent the types of activities in each category. MOREnet members and affiliates may:

1. Generate revenue for services to recover the costs of the service.

2. Accept donations from individuals and commercial enterprises.

3. Community networks may establish different level of membership based on donations and use services as a reward or incentive for higher donations.

4. Perform fund raising activities that benefit the member/affiliate or provide a basis for additional services, i.e., larger modem pool, SLIP/PPP access, added server memory.

5. Promote business in general, i.e., economic development or tourism, but not promote an individual business. Promoting a particular industry is permissible provided the activity does not focus on an individual company or companies of the industry to the exclusion of other. For example, a community may promote tourism and resorts, but not promote ABC Resort and DEF Resort to the exclusion of other resorts.

6. Place a company logo on a public information web page sponsored by that company. Provide a list of commercial enterprises in the community, i.e., Chamber of Commerce business listing as a public service. Such business listing could include address and phone number and a brief description of the product or service offered by the business. The format and depth of coverage should be consistent throughout the list.

7. Hot link from company logos or Chamber business listing to company homepages on a commercial Internet service.

8. Perform services that have a valid public interest and fit within the MOREnet charter of research, education, and public information.

9. Place public access workstations/kiosks in commercial establishments provided they are actually accessible to the public, i.e., placing a kiosk in a shopping center courtyard.

10. Issue e-mail accounts to businesses for public purposes; i.e., school-business partnership program or media accounts for publicizing community activities.

11. Universities may establish a business incubator that houses for-profit companies, provided the business incubator is a planned component that is in alignment with the University's mission statement. A typical plan for this type of incubator would be expected to have guidelines for the types of companies housed and parameters on usage of the incubator's services. Typical parameters would include: the length of time a company would be housed in the incubator, boundaries on the use of the facility's services (including the MOREnet Internet1 connection) and an adjunct appointment for the company staff. When a company is no longer eligible to be housed within the incubator, it would no longer be eligible to receive access to MOREnet services (MOREnet, 2006).

Examples for MOREnet not to follow. MOREnet members and affiliates may not:

1. Sell access (as previously mentioned, cost recovery processes are permissible).

2. Sell homepages to commercial enterprises.

3. House homepages/websites of commercial enterprises.

4. Promote individual businesses.

5. Permit commercial enterprises to sell/advertise though a MOREnet connection/server.

6. Sell/provide e-mail accounts to aid commercial activities; including listing e-mail accounts on business cards.

7. Provide links or lists of commercial enterprises on a fee basis; i.e., pay a fee to the member/affiliate to get your business listed in a directory (MOREnet, 2006).

In comparing differences in policies between UND and UMKC, a realization was made that these entities follow different sets of guidelines in regards to the audiences served. UND follows NDUS policies that set procedure for all computer operations within the state's higher educational institutions. However UMKC set their policies for a wider base of customers, including businesses and hospitals. Thus there are more differences between the two institutions than similarities.

Similarities include Acceptable Use Policies, Intellectual Property, Virus, Privacy Rights, Business Related Violations, Security / Firewall, Reporting Misuse, Risk Assessment and Incident Response Team. Differences consist of Unauthorized Use, Interdepartmental Policies, Copyrights, Hacking, Harassment, Inappropriate Use, Wasting Resources, Threats, Anonymous Identity, Damage Resources, Consequences/Appeals, and the emerging problem of defining Commercial Activities.

Summary

Chapter IV consisted of analyzing the security policies gathered from the University of North Dakota and University of Missouri at Kansas City. The data was categorized under two general headings of similarities and differences found in the policies.

NDUS and MOREnet have sets of polices for their state universities plus each university has individual institution polices to cover their vast computer concerns. In order to be able to adequately support each separate entity within the university, a system of authority has been put in place to create policies regarding these technologies. Individual policies are tailored to protect university ongoing and growing threats in a field where new technologies emerge. The next chapter reports the final results and conclusions of this study.

CHAPTER V

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

Summary

The purpose of this study was to examine and analyze the computer security policies of two benchmark universities to determine both similarities and differences. The specific goal was to gather information to help determine improvements in computer security policy implementation from two universities. The overall goal of this study was to examine the computer security policies of two higher education institutions and do a comparison to search for gaps or areas that are not protected by policy for each university, with the intent to aid the writing of future computer security policies to protect vulnerabilities discovered.

Chapter II is the literature review that contains the scholarly literature. That investigation helped the researcher to limit the scope of the inquiry, and to express the importance of studying a topic to readers. It shared with the reader the results of other research closely related to the topic.

Chapter III included an explanation of how the method of analysis was used. It was followed by an explanation of the procedures including data collection and coding process. The chosen research method was a content analysis; this consisted of collecting data, breaking it down into two categories comparing similarities and differences. An analysis of these computer policies was necessary to recognize gaps determining whether or not policies address pertinent contemporary computer security issues.

Chapter IV consisted of analyzing the computer security policies gathered from the two institutions being studied. This data was then examined and compared to determine the information that the policies were written to represent.

Conclusions

This study showed the similarities and differences in policies that were implemented for two higher educational institutions. Both higher education institutions are under the umbrella of policies from a higher authority, UND falls under NDUS whereas UMKC is under MOREnet.

While completing this study and identifying similarities between the two institutions it was discovered that NDUS does not have an acceptable use policy identified directly but rather the information is covered in a general manner throughout the policies. However MOREnet does have acceptable use identified, but not in as much detail. In comparing intellectual property policies it was discovered that NDUS has covered this area in detail while MOREnet does not touch on this topic beyond a brief mention. Regarding the ever-present danger of virus attacks NDUS does a good job of covering this area while MOREnet gives a shorter description of prohibitions. Concerning privacy rights NDUS includes much more detail on their policy compared to MOREnet. Business-related violations policy was addressed in NDUS policy, however MOREnet' extensive list covered a wider variety of possible situations. Security/firewall policies were similar for both institutions. The procedure for reporting misuse is not directly identified in the NDUS policy; MOREnet does a very thorough job at identifying and covering this area. The risk assessment policy is covered thoroughly by MOREnet while UND is in the development stages of setting up a policy and team.

An incident response team is currently being put together by UND's Chief Security Officer (CSO). The direction of this team and the education of its staff is the responsibility of the CSO at UND. The incident response team for MOREnet reports all of their incidents to their university CERT.

Recommendations

The following recommendations are provided to all computer security policy writers as well as technology users. The recommendations are relevant to all universities. It can be determined that each organization, regardless of private or public, should have the opportunity to write policies for their individual needs. It also can be determined that there must be room to alter policies as needed. As technology grows, so do new challenges that follow. It is important to realize that with rapid increase of new technology there are more challenges to contend with.

The Need for Clear and Concise Language

After examining all of the information between the two higher education institutions, it is recommended for the University of North Dakota to directly elaborate and identify an acceptable use policy. University of Missouri at Kansas City has already identified this directly with a heading before the policy that explains it. The information of acceptable use is identified indirectly but it is not identified with a title. The policies should have clear and concise headings and should be identified in the policy.

Further Development of Unauthorized Use Policy

UMKC needs more policies concerning harassment, hacking and unauthorized use; topics that are not identified in their policies. Individuals who use University of North Dakota computer facilities assume the responsibility of seeing that these resources are used in the appropriate manner. Misuse of computer facilities is considered a violation of University policy and regulations and may also be a violation of law if data of other computer users are disturbed or the privacy rights of individuals are violated.

Specific student use policies

Educational institutions should have policy guidelines specifically written for students. UND's Code of Student Life mentions very specific actions that will be taken if students violate their computer policies. They are different from the writing of NDUS policies. For example, the list mentions chain letters, an activity that is specifically prohibited because it uses and detracts from resources. UMKC does not have similar policies available to their students.

High-profile publication of policies

UND lists computer policy violations in its Code of Student Life. Each student receives a copy of the publication. This is a good way to address students who may seek opportunities to cause disruptions. All education institutions could and should implement this manner of publication.

The use of peer-to-peer software sharing

Every educational institution should write a policy to protect their networks from peer-to-peer software sharing applications. This software is unsafe and can be associated with viruses and spy ware.

Effective appeals processes

UMKC needs to have an appeal process implemented into the policy listings. Violation of the acceptable use policy may result in denial of access to university computer resources in disciplinary actions provided or authorized by the Collected Rules and Regulation of the University of Missouri. Violations of acceptable use policy that are not promptly remedied by the member institution or project participant may result in termination of the service or membership, thus it is imperative that mistaken actions be addressed as soon as possible.

Ongoing risk assessment

UMKC and UND need to have a policy regarding risk assessments of information systems infrastructure and data to help discover vulnerabilities. This must be an ongoing process, with a committee set up to re-visit the matter at least once a year.

The need for CERT

Where one does not exist it is necessary to create an incident response team to go beyond administrative duties to respond to infringement of acceptable use, violations of the law, dealing with compromised hosts/servers, and major incidents involving loss of sensitive or protected data. Each institution should have an incident response team composed of information technology employees from across the institution in place to handle any problems with protecting the network systems, solving problems as they arise.

Incidence tracking

A tracking system is necessary for follow-up on incidences as they occur, this is important for all institutions to have this. Tracking must be an ongoing process, dealing with problems as they arise so they can be categorized by severity and archived.

Reporting misuse

A policy must be put in place for reporting technology misuse with enforcement of penalties. UND lists the duties of campus computer officials including the Campus Information Technology Security Officer, the Campus Judicial Officers and the Chief Information Officer, and their given responsibilities. UMKC does not provide this information on their Web site.

Policy for researching domain names

UND should have policy implemented to create forms for requesting published Domain Name Service (DNS) for web servers and e-mail post office domains. This is something that ought to be addressed as it will save time and money wasted by unnecessary research.

The Human Aspect

After analyzing the information gathered, this study has shed new light about the creation of policies. In the interest of protecting the technology system and guiding its use we cannot forget the human aspect. Responsibility must be exercised by the user to respect the needs of others in the process. Data security, hacking and harassment can all be involved in the misuse of technology and cause distress to an individual and institutions, whether it be by disrupting an ongoing research project, stealing identities or bothering others unnecessarily. These recommendations are offered for UMKC and UND in order to put needed policies into place for technology to be utilized to the full and for the advantages gained to be shared and enjoyed by all.

Limitations

Lack of Current Information

On the whole Web sites were not updated. At the start of the study, data on policies were gathered from the websites of UND, NDUS, UMKC and MOREnet. UMKC has since updated certain policies on its Web site, but not all of them.

The institutions studied are rewriting policies in an ongoing process. During the course of the study, communication with institutional policy writers indicated more new policies are on the way.

Differences in Policy Application

Each institution has different policy priorities. Both institutions provide services for different users. MOREnet policies are written for a broader base of clientele. They cover the private sector and appear more adapted with MOREnet's responsibilities to the customers whereas NDUS policies are written for user to user interaction. For example, NDUS addresses the issue of stealing intellectual property of one user from another. MOREnet is more concerned with a client's property rights being intellectually violated by other users on their system.

Sample Size

This study's primary limitation is that it does not encompass a larger pool of subjects. Because technology priorities differ, peer universities face problems of technological expansion and may not as easily adapt as a larger university. However if larger institutions were included in this study, their policies could pinpoint areas of future technological challenges to the smaller institutions. Also, an increase in the number of subjects involved in the study increases the pool of information necessary to find and test new ideas.

Universities and colleges are the testing ground for new technologies, making them the ideal research subject, however the need for flexibility leaves these technologies open to unauthorized use. Effective computer policy becomes ever more essential as our ability to conquer new territory in human communication grows. Real dangers coexist with the promising advances of each new discovery. The future role of higher education as leader in technological innovation may largely depend on the answers found to today's questions. With so much at stake, we cannot afford to fail.

APPENDICES

APPENDICES

APPENDIX A: NDUS COMPUTER USE POLICY

Definitions

Authorized use

Use of computing and networking resources shall be limited to those resources and purposes for which access is granted. Use for political purposes is prohibited (see Section 39-01-04 of the ND Century Code). Use for private gain or other personal use not related to job duties or academic pursuits is prohibited, unless such use is expressly authorized under governing institution or system procedures, or, when not expressly authorized, such use is incidental to job duties or limited in time and scope, and such use does not: (1) interfere with NDUS operation of information technologies or electronic mail services; (2) burden the NDUS with incremental costs; or (3) interfere with the user's obligations to the institution or NDUS.

Authorized user(s)

Computing and networking resources are provided to support the academic research, instructional, outreach and administrative objectives of the NDUS and its institutions. These resources are extended to accomplish tasks related to the individual's status with NDUS or its institutions. Authorized users are (1) current faculty, staff and students of the North Dakota University System; (2) individuals connecting to a public information service (see section 5.3); and (3) other individuals or organizations specifically authorized by the NDUS or an NDUS institution. For the purposes of this policy, no attempt is made to differentiate among users by the user's group. These policies treat all users similarly, whether student, faculty, staff or other authorized user, in terms of expectations of the user's conduct.

Campus IT Department

Official central information technology department as designated by the institution's president or chief executive officer.

Campus Information Technology Security Officer

Individual, designated by the Institution, responsible for IT security policy education and enforcement, and coordination of incident investigation and reporting.

Campus Judicial Officers

The designated Campus Judicial Officers for students, or appropriate supervising authority for faculty and staff, as defined by the Institution.

NDUS Chief Information Officer Council representative (CIO)

The senior staff member responsible for information technology.

Computing and networking resources

Computing resources and network systems including, but not limited to, computer time, data processing, and storage functions; computers, computer systems, servers, networks, and their input/output and connecting devices; and any related programs, software and documentation. Further, it is understood that any device that connects to a campus network, whether wired or wireless, is expected to comply with all NDUS and institutional policies and procedures.

Electronic information

Any electronic text, graphic, audio, video, digital record, digital signature or message stored on or transported via electronic media. This includes electronic mail messages and web pages.

HECN

The North Dakota Higher Education Computer Network, which has been given the responsibility of maintaining the computer and network systems for the North Dakota University System.

Institution

One of the eleven colleges or universities within the North Dakota University System.

Open record

Electronic information used in support of college, university or NDUS business, regardless of where the electronic information originated or resides may be subject to open records laws of North Dakota (see Section 44-04-18 of the ND Century Code).

Scrubbed

The act of ensuring that no data is retrievable from a storage device according to current "best practice."

Sensitive data

Any data, the unauthorized disclosure of which may place the Institution or NDUS at risk.

Server

Any device that provides computing service to multiple computers or individuals.

Student record

As defined by the Family Educational Rights and Privacy Act of 1974 (FERPA), a student educational record includes records containing information directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution.

Unit

Department, office or other entity within an institution.

Update

A new release (or version) or a piece of software that is generally understood to be an error correction release and does not contain new functionality.

Upgrade

A new release (or version) of a piece of software that contains new functionality.

User

See Authorized User(s)

Individual Privileges

The following individual privileges are conditioned upon acceptance of the accompanying responsibilities within the guidelines of the Computer and Network Usage Policy.

2.1 Privacy

In general, all electronic information shall be free from access by any but the authorized users of that information. Exceptions to this basic principle shall be kept to a minimum and made only when essential to:

1. Meet the requirements of the state open records law and other statutory or regulatory requirements.

2. Protect the integrity of the College or University and the rights and property of the State.

3. Allow system administrators to perform routine maintenance and respond to emergency situations such as combating "viruses" and the like (see 4.3, 4.4).

2.2. Encryption and password protection

When using encryption utilities or password protection schemes on institutional information or computing equipment, a unit-level recovery process must be used. No data protection schemes may be used to deprive a unit or institution from access to data or computing equipment to which they are entitled.

2.3. Freedom from harassment and undesired information

All members of the campus community have the right not to be harassed by computer or network usage of others (see 3.1.3.).

2.4. Appeals of sanctions

Individuals may appeal any sanctions according to the process defined for their Institution.

Individual Responsibilities

Each member of the campus community enjoys certain privileges and is responsible for the member's actions. The interplay of these privileges and responsibilities engenders the trust and intellectual freedom that form the heart of this community.

3.1. Respect for rights of others and legal and policy restrictions

Users are responsible to all other members of the campus community in many ways. These include the responsibility to:

1. Respect and value the right of privacy.

2. Recognize and respect the diversity of the population and opinion in the community.

3. Comply with NDUS and Institution policy and all laws and contracts regarding the use of information that is the property of others.

3.1.1 Privacy of information

All electronic information which resides on NDUS and institution computers, and any data on any device that connects, wired or wireless, to the campus network may be determined to be subject to the open records laws of North Dakota.

Individuals are prohibited from looking at, copying, altering, or destroying another individual's electronic information without explicit permission (unless authorized or required to do so by law or regulation). The ability to access a file or other information does not imply permission to do so unless the information has been placed in a public area such as a web site.

The NDUS CIO is authorized to develop and publish standards for the NDUS institutions. The NDUS Data Classification and Information Technology Security Standard further defines and explains NDUS and institution data classifications, standards, and security responsibilities.

Except to the extent that a user lacks control over messages sent to the user, electronic information is deemed to be in the possession of a user when that user has effective control over the location of its storage.

3.1.2 Intellectual property

Users are responsible for recognizing and honoring the intellectual property rights of others. Users are prohibited from using, inspecting, copying, storing, and redistributing computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) intentionally using the computer to contact another person repeatedly with the intent to annoy, harass or bother, whether or not an actual message is communicated, and/or the purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease; (3) intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right or institutional sanction to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease; (4) intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another; or (5) Intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

3.2. Responsible use of resources

Users are responsible for knowing to which resources they have been granted access, and refraining from all acts that waste or prevent others from using these resources, or from using them in ways proscribed by the NDUS or NDUS institutions or state or federal laws.

3.3. Information integrity

Electronic information is easily manipulated. It is the user's responsibility to verify the integrity and completeness of information compiled or used. No one should depend on information or communications to be correct if the information or communication is contrary to expectations. It is important to verify that information with the source.

3.4. Use of personally managed systems

Any device connecting directly to a NDUS or institution network, whether via wire or wireless or modem device must be administered and maintained in a manner consistent with the policies of the NDUS and institution and all applicable laws, including access and security issues. Anti-virus software should be installed and any software installed (especially operating system and anti-virus software) should be kept up-to-date with regard to security patches.

Personal firewalls should be deployed when their installation will not interfere with the function of the device or the administration of the network; and such firewalls should be configured to allow minimal traffic.

At a minimum, password facilities should be utilized to ensure that only authorized individuals can access the system.

Passwords should be a minimum of eight characters and a combination of upper and lower case letters, numbers and special characters, as the system allows. They should not be words found in a dictionary. Nor should they be something that is easily discerned from knowledge of the owner. Passwords should not be written anywhere and not sent via email or shared with others. System administrators will ensure that passwords are not readable in plain text on the systems.

The administrative account/login and password should be changed to values specified by the campus IT department; and any system default "guest" account/login should be assigned a password and disabled.

All unnecessary software and services should be disabled.

Any device configured as a server must be registered with the campus IT department.

The NDUS CIO is authorized to develop and publish standards for the NDUS institutions. The NDUS Server Information Technology Security Standard further defines NDUS and institution server standards and security responsibilities.

It is the responsibility of the owner/administrator of a personally managed system to maintain logs appropriate to the type of server and to make those logs available to NDUS or institution personnel as needed.

The HECN manages the name space and IP subnets for the NDUS. Policies pertaining to these services can be found at http://www.ndus.nodak.edu/uploads/document-library/835/1901.2-DNS.PDF

3.4.1 Video transmission devices

All audio and/or video transmission devices (web cams, etc.) must be utilized in a manner consistent with these policies and all applicable laws.

3.5. Access to computing and networking resources

The NDUS makes every effort to provide secure, reliable computing and networking resources. However, such measures are not foolproof and the security of a user's electronic information is the responsibility of the user.

Administrative desktop computers should be behind locked doors when the office is unoccupied and access to these devices should be based on minimal need.

Under no circumstances may an external network be interconnected to act as a gateway to the campus network without coordination and explicit approval from the campus IT department.

3.5.1 Sharing of access

Access to computing and networking resources, computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. Users are responsible for any use or misuse of their authentication information and authorized services.

Institution Departments or Administrative Offices; or Institution-wide Help Desk or information functions; or officially recognized Faculty, Staff or Student Organizations may be granted permission for multi-user accounts with common authentication, for approved purposes. Requests for these types of accounts must come from the individual assuming responsibility for the activity of the account and be approved by the NDUS Chief Information Officer Council representative. Only the person responsible for the activity of the account is authorized to share access and authentication information and only persons individually entitled to access NDUS systems may be given access to these accounts.

3.5.2 Permitting unauthorized access

Authorized users may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users (see section 1).

3.5.3 Use of privileged access

Access to information should be provided within the context of an authorized user's official capacity with the NDUS or NDUS institutions. Authorized users have a responsibility to ensure the appropriate level of protection over that information.

3.5.4 Termination of access

When an authorized user changes status (e.g., terminates employment, graduates, retires, changes positions or responsibilities within the Institution, etc.), the user must coordinate with the unit responsible for initiating that change in status to ensure that access authorization to all institution resources is appropriate. A user may not use computing and networking resources, accounts, access codes, privileges, or information for which the user is not authorized.

3.5.5. Backups

While the NDUS will make every effort to provide reliable computing facilities, ultimately it is the individual user's responsibility to maintain backups of their own critical data. Such backups should be stored in a secure off-site location.

3.5.6 Device registration

Any desktop computer and any network addressable device that connects to a campus network should be approved by and registered with the campus IT department.

3.6. Attempts to circumvent security

Users are prohibited from attempting to circumvent or subvert any system's security measures. Any security incidents should be reported to the system administrators and the Campus IT Security Officer.

3.6.1 Decoding access control information

Users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

3.6.2. Denial of service

Deliberate attempts to degrade the performance of any computer system or network or to deprive authorized personnel of resources or access to any computer system or network are prohibited.

3.6.3 Harmful activities

Harmful activities are prohibited. Examples include, but are not limited to, IP spoofing; creating and propagating viruses; port scanning; disrupting services; damaging files; or intentional destruction of or damage to equipment, software, or data.

3.6.4. Unauthorized activities

Authorized users may not:

1. Damage computer systems;
2. Obtain extra resources not authorized to them;
3. Deprive another user of authorized resources
4. Gain unauthorized access to systems by using knowledge of a special password; loopholes in computer security systems; another user's password, or access abilities used during a previous position.

3.6.5. Unauthorized monitoring

Authorized users may not use computing resources for unauthorized monitoring or scanning of electronic communications without prior approval of the campus CIO or the campus or NDUS IT Security Officer.

3.7. Academic dishonesty

Use of NDUS computing facilities to commit acts of academic dishonesty will be handled through existing campus procedures which address allegations of academic dishonesty.

3.8. Personal business

Computing and networking resources may not be used in connection with compensated outside work or for private business purposes unrelated to the NDUS or institutions, except in accordance with the NDUS Consulting Policy.

NDUS and NDUS Institution Privileges

4.1. Control of access to information

NDUS and NDUS institutions may control access to their information and the devices on which it is stored, manipulated, and transmitted, in accordance with the policies of the Institution and NDUS and federal and state laws. Access to information and devices is granted to authorized NDUS personnel as necessary for the performance of their duties and such access should be based on minimal need to perform those duties.

4.2. Imposition of sanctions

The Institution may impose sanctions on anyone who violates the Computer and Network Usage Policy.

4.3. System administration access

A system administrator (i.e., the person responsible for the technical operation of a particular machine) may access electronic information as required for the maintenance of networks and computer and storage systems, such as to create backup copies of media. However, in all cases, all rights to privacy of information are to be preserved to the greatest extent possible.

4.4. Monitoring of usage, inspection of electronic information

The Electronic Communications Privacy Act allows system administrators or other authorized campus and NDUS employees to access a person's electronic information in the normal course of employment, when necessary, to protect the integrity of computing and networking resources or the rights or property of the Institution or NDUS. Additionally, other laws, including the U.S.A. P.A.T.R.I.O.T. ACT of 2001, may expand the rights and responsibilities of campus administrators. Electronic information may be subject to search by law enforcement agencies under court order.

The NDUS and Institution may also specifically monitor the activity, systems and accounts of individual users of the Institutions' computing and networking resources without notice. This includes individual login sessions, electronic information and communications. This monitoring may occur in the following instances:

1. The user has voluntarily made them accessible to the public.
2. It reasonably appears necessary to do so to protect the integrity, security, or functionality of the Institution or to protect the Institution or NDUS from liability.
3. There is reasonable cause to believe that the user has violated, or is violating, Institution or NDUS policies or any applicable laws.
4. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns.
5. Upon receipt of a legally served directive of appropriate law enforcement agencies.
6. Upon receipt of a specific complaint of suspected or alleged violation of policy or law regarding a specific system or activity.

Any such monitoring must be accomplished in such manner that all privileges and right to privacy are preserved to the greatest extent possible and with the prior permission of the Campus ITSO or CIO, if reasonable.

For further information, please see 2.1 for information on privacy.

4.5 Suspension of individual privileges

NDUS and Institutions operating computers and networks may suspend computer and network privileges of a user:

1. To protect the integrity, security or functionality of the Institution or NDUS and/or their resources or to protect the Institution or NDUS from liability;

2. To protect the safety or well-being of members of the community;

3. Upon receipt of a legally served directive of appropriate law enforcement agencies or others.

Access will be promptly restored when the protections are assured, unless access is suspended as a result of formal disciplinary action imposed by Campus Judicial Officers, HECN or other legal officers.

4.6 Retention of access

User accounts are assigned to a specific individual at a specific institution within the NDUS. When a specific affiliation is terminated, the NDUS or Institution may elect to terminate the user's account, transfer the account, continue the account for a limited period of time, or, in the case of e-mail, temporarily redirect incoming communications.

4.7 Network maintenance

The HECN and the campus networking personnel have the responsibility of maintaining the networks for the benefit of all authorized users. This implies that, in emergency situations, they may, if there is no other way to resolve a problem, request that a device (whether wired or wireless) be disconnected from the network or powered down, or, if necessary, take such action themselves.

accidents and deliberate attempts to damage the systems.

The NDUS CIO is authorized to develop and publish standards for the NDUS institutions. See NDUS Physical Information Technology Security Standards for additional information.

5.1.2. Configuration concerns

The Institution's campus IT department shall, for those desktops they manage, change the Administrative login and password, make inaccessible any system defined accounts and turn off any unnecessary software or services. Any access to a server, other than a public server, should be authenticated and logged. Access to all servers should be based on minimal need.

Software with security vulnerabilities will be patched in a timely manner.

The NDUS CIO is authorized to develop and publish standards for the NDUS institutions. Refer to the NDUS Server Information Technology Security Standard for more information.

5.2. Security procedures

The NDUS and Institutions have the responsibility to develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity of individual and institutional computing and networking resources, and to impose appropriate sanctions when security or privacy is abridged.

Each Institution shall designate an Information Technology Security Officer to coordinate the security efforts on their campus. This individual shall be considered an "other school official" determined to have legitimate educational interests for purposes of sharing information under federal law. This person shall coordinate efforts and share information, with other campus officials, as necessary. The Information Technology Security Officer will keep appropriate records of any incidents/investigations on the Officer's campus and, if requested, share those records with the appropriate NDUS personnel.

The NDUS shall designate an Information Technology Security Officer, who will assist the campus Information Technology Security Officers in their duties and who shall be considered an "other school official" determined to have legitimate educational interests for each campus under federal law.

5.3. Public information services

Institutions may configure computing systems to provide information services to the public at large. (Current examples include, but are not limited to "ftp" and "www") However, in so doing, any such systems must comply with all NDUS and institution policies and applicable laws. Particular attention must be paid to the following sections of this policy: 1(Authorized use), 3.1.2 (Intellectual Property) and 3.2 (Responsible use of resources). Use of public services must not cause computer or network loading that impairs other services or impedes access.

5.4 Communications and record keeping

It is the responsibility of each institution that provides computing facilities to: inform users of all applicable NDUS computing policies and procedures; to address, through existing campus judicial procedures any resulting complaints to maintain appropriate records and to inform the NDUS CIO designate of the progress and resolution of any incident responses; and provide an environment consistent with these policies and procedures.

5.5 Backup and retention of data

Normal backup procedures are employed for disaster recovery on NDUS and institution systems. Therefore, if a user removes electronic information, it may still be retrievable by the system administrators. These backups may or may not be retained for an extended period of time. Backed-up electronic information may be available for the investigation of an incident by system administrators or law enforcement personnel. Administrators of the systems may be required to attempt to recover files in legal proceedings.

For data critical to the function of the Institution, a second set of backups should be maintained off-site in a secured protected area.

5.6 Schedule of service

Most scheduled maintenance of NDUS computing and networking resources will be done at pre-announced times. There are times when some computing and networking resources will be unavailable due to unforeseeable circumstances. Problems may arise with electronic information transmission and storage. Such occurrences may cause a disruption to service or loss of data. The NDUS assumes no liability for loss of service or data. However, all efforts must be made to ensure the availability of services at other than scheduled maintenance times.

5.7 Privacy of records

Campus access to student computer records will be governed by existing campus records policies. Generally, student records, including computer records, fall under the Family Educational Rights and Privacy Act of 1974 (FERPA). The computer records of a student are educational records and cannot be released without written consent from the student except as elsewhere defined by institutional policy or state or federal law. The institution's response to subpoenas for student records will be carried out as defined by the institution and state or federal law.

The NDUS CIO is authorized to develop and publish standards for the NDUS institutions. Standards for institutional data and its classifications can be found in the NDUS Data Information Technology Security Standard.

5.8 Domain name services

The HECN administers the nodak.edu domain and IP subnets for NDUS. Procedures for adding hosts and related policies can be found in the "Policy for Name Service and Usage"

5.9 Virus protection software

The HECN shall make available virus-protection software for NDUS users and keep available the most current updates.

5.10 Legal software

The Institution shall periodically audit institutionally owned devices for proper software licenses.

5.11 Data privacy

Any electronic data asset of the NDUS or the Institution shall be classified as Public, Private or Confidential according to the NDUS Data Information Technology Security Standard.

The owner of data is that person, department or office that is responsible for the integrity of the data. It is the responsibility of the owner of the data to classify the data.

It is the responsibility of anyone using or viewing the data to protect the data at the level determined by the owner of the data or as mandated by law.

Appropriate efforts must be taken to ensure data integrity, confidentiality and availability.

PROCEDURES AND SANCTIONS

The NDUS makes every reasonable effort to protect the rights of the individual users of its computing and networking resources while balancing those rights against the needs of the entire user community. The NDUS and Institution will make every effort to resolve any system or network problems in the least intrusive manner possible.

6.1. Investigative contact

If anyone is contacted by a representative from an external law enforcement organization (District Attorney's Office, FBI, ISP security officials, etc.) that is conducting an investigation of an alleged violation involving NDUS or Institution computing and networking resources, they must inform the Institution's Information Technology Security Officer and the NDUS Information Technology Security Officer.

6.2. Responding to security and abuse incidents

All authorized users are stakeholders and share a measure of responsibility in intrusion detection, prevention, and response. In the NDUS, the HECN has been delegated the authority to enforce information security policies and is charged with: Implementing system architecture mandates, system protection features, and procedural information security measures to minimize the potential for fraud, misappropriation, unauthorized disclosure, loss of data, or misuse.

Initiating appropriate and swift action, using any reasonable means, in cases of suspected or alleged information security incidents to ensure necessary protection of NDUS or an Institution's resources, which may include disconnection of resources, appropriate measures to secure evidence to support the investigation of incidents, or any reasonable action deemed appropriate to the situation.

All users and units have the responsibility to report any discovered unauthorized access attempts or other improper usage of NDUS or Institution computing and networking resources. All users and units that have reported to them (other than as in 6.1 above) a security or abuse problem with any NDUS or Institution computing or networking resources, including violations of this policy are to:

Take immediate steps as necessary to ensure the safety and well being of information resources. For example, if warranted, a system administrator should be contacted to temporarily disable any offending or apparently compromised computer accounts, or to temporarily disconnect or block offending computers from the network (see section 4.5, 4.6 and 4.7).

Make appropriate reports on any discovered unauthorized access attempts or other improper usage of institution or NDUS computing and networking resources.

Ensure that the following people are notified: (1) The administrator of the computer, if known. (2) If appropriate, the campus Information Technology Security Officer or the campus IT Department.

6.3. First and minor incident

Minor infractions of these policies are generally resolved informally by the unit administering the accounts or network in conjunction with the Campus Information

Technology Security Officer. Minor infractions are those in which the impact on the computer or network resource is minimal and limited to the local network. Resolution of the infraction will include referral to the Code of Student Life, staff or faculty handbooks, or other resources for self-education about appropriate use. In the case of students, a copy of the resolution will be sent to the Campus Judicial Officer.

6.4. Subsequent and/or major violations

Repeated minor infractions or more serious misconduct may result in immediate loss of computer access privileges or the temporary or permanent modification of those privileges. More serious violations include, but are not limited to, unauthorized use of computing facilities, attempts to steal passwords or data, unauthorized use, distribution or copying of licensed software, or other copyrighted materials, use of another's account, harassment or threatening behavior, or crashing the system. Policy violators will be referred by the campus Information Technology Security Officer to the Campus Judicial Officer for further action.

6.5. Range of disciplinary sanctions

Users who violate this policy are subject to the full range of sanctions, including the loss of computer or network access privileges, disciplinary action, dismissal from the institution, and legal action. Use that is judged excessive, wasteful, or unauthorized may result in denial of access to computing and networking resources and may subject the user to appropriate disciplinary and/or legal procedures. Any offense which violates local, state, or federal laws may result in the immediate loss of all computing and networking resource privileges and will be referred to appropriate college or university offices and/or law enforcement authorities.

6.6. Appeals

Notice of violations and appeals of decisions will follow campus procedures.

APPENDICES
APPENDIX B: MOREnet POLICY AND PROCEDURES

Acceptable Use Policy

Acceptable Use

All network use by MOREnet members, project participants and those connected via MOREnet members or project participants shall be for, or in support of, research; education; local, state or national government affairs; economic development or public service.

Unacceptable Use

It is not acceptable to use MOREnet for purposes which violate federal or state law.

It is not acceptable to use MOREnet for any purpose which violates the intellectual property rights of others.

It is not acceptable to use MOREnet in a manner that intentionally or negligently disrupts normal network use and service. Such disruption would include the intentional or negligent propagation of computer viruses, the violation of personal privacy, and the unauthorized access to protected and private network resources.

It is not acceptable to use MOREnet for commercial activities that are not in support of education, research, public service, economic development or government purposes. Further, it is not acceptable to distribute unsolicited advertising. Additional information regarding unacceptable commercial uses of MOREnet is available.

Enforcement of Policy

Each MOREnet member or project participant must make reasonable efforts to publicize the policies of MOREnet and to ensure compliance of those connected through them.

Reported and perceived violations of the Acceptable Use Policy will be reviewed by the MOREnet Executive Director. Violations that are not promptly remedied by the member institution or project participant may result in action including the termination of MOREnet service or the forfeiture of MOREnet membership.

Questions

If you have questions about the MOREnet Acceptable Use Policy, its interpretation or enforcement, please send e-mail to security@more.net.

Policies and Procedures

Non-Commercial Use Explanation

MOREnet Mission Statement. The primary mission of MOREnet is to provide collaborative networked information services to its member/customers in support of education, research, public service, economic development and government.

MOREnet Acceptable Use Policy Statement

It is not acceptable to use MOREnet for commercial activities, including, but not limited to, commercial solicitation of business.

Defining Commercial Activities

Commercial activity means that you may not sell connections, advertise commercial products using a MOREnet connection or MOREnet provided/managed server, sell products or services directly through using a MOREnet connection or

MOREnet provided/managed server, or provide electronic mail accounts for the furtherance of commercial activities as noted above.

Examples

The following lists of permissible and prohibited activities are not exhaustive, but merely represent the types of activities in each category.

MOREnet members and affiliates may:

1. Generate revenue for services to recover the costs of the service.

2. Accept donations from individuals and commercial enterprises.

3. Community networks may establish different level of membership based on donations and use services as a reward or incentive for higher donations.

4. Perform fund raising activities that benefit the member/affiliate or provide a basis for additional services, i.e., larger modem pool, SLIP/PPP access, added server memory.

5. Promote business in general, i.e., economic development or tourism, but not promote an individual business. Promoting a particular industry is permissible provided the activity does not focus on an individual company or companies of the industry to the exclusion of other. For example, a community may promote tourism and resorts, but not promote ABC Resort and DEF Resort to the exclusion of other resorts.

6. Place a company logo on a public information web page sponsored by that company.

7. Provide a list of commercial enterprises in the community, i.e., Chamber of Commerce business listing as a public service. Such business listing could include address and phone number and a brief description of the product or service offered by the business. The format and depth of coverage should be consistent throughout the list.

8. Hot link from company logos or Chamber business listing to company homepages on a commercial Internet service.

9. Perform services that have a valid public interest and fit within the MOREnet charter of research, education, and public information.

10. Place public access workstations/kiosks in commercial establishments provided they are actually accessible to the public, i.e., placing a kiosk in a shopping center courtyard.

11. Issue e-mail accounts to businesses for public purposes; i.e., school-business partnership program or media accounts for publicizing community activities.

12. Universities may establish a business incubator that houses for-profit companies, provided the business incubator is a planned component that is in alignment with the University's mission statement. A typical plan for this type of incubator would be expected to have guidelines for the types of companies housed and parameters on usage of the incubator's services. Typical parameters would include: the length of time a company would be housed in the incubator, boundaries on the use of the facility's services (including the MOREnet Internet1 connection) and an adjunct appointment for the company staff. When a company is no longer eligible to be housed within the incubator, it would no longer be eligible to receive access to MOREnet services.

MOREnet members and affiliates may not:

1. Sell access (however, cost recovery processes are permissible).

2. Sell homepages to commercial enterprises.

3. House homepages/websites of commercial enterprises.

4. Promote individual businesses.

5. Permit commercial enterprises to sell/advertise though a MOREnet connection/server.

6. Sell/provide e-mail accounts to aid commercial activities; including listing e-mail accounts on business cards.

7. Provide links or lists of commercial enterprises on a fee basis; i.e., pay a fee to the member/affiliate to get your business listed in a directory.

Special Case for Health Care Facilities

There is a compelling public interest in facilitating the delivery of health care information and resources via electronic means to the public. Health care facilities are in an industry that is completely mixed between public and private enterprise. The Department of Health has responsibility for licensing and oversight of health care facilities within the state. Local communities rely heavily on health care facilities as an essential element of the community. Involvement of health care facilities in a community network will also provide an enhanced communications capability among citizens, health care providers, and the Department of Health. Considering these facts, health care facilities, regardless of whether they are publicly or privately funded, may be included as partners in community networks without violating the non-commercial use policy. The special case will apply provided that the health care facility does not directly engage in commerce; i.e., advertising, selling services, etc. through their connection. Valid public information services are appropriate and adherence to the non-commercial use rule can be measured against this standard. Services to individual physicians' offices are not permitted under this special case. (Physicians may have community network accounts, subject to the same benefits and restrictions as any other citizen.)

Conclusion

MOREnet customers expect MOREnet to be aware of security issues and to respond to security incidents on their behalf. The number of customers seeking MOREnet response will continue to grow, as will the level of service required by customers, as concerns over security and actual compromises in security increase.

To meet these growing needs and expectations, MOREnet has identified three services addressing Internet security:

A. Security Incident Response Team — Provide response for MOREnet customers to security incidents involving system, server or network infrastructure attacks or compromises.

B. Security Consulting — Provide MOREnet customers with advice and recommendations for general security implementations for their local network servers, infrastructure and procedures.

C. Internet Security Training/Seminars — Conduct and sponsor training sessions or seminars on Internet security topics, best practices and specific technologies such as firewalls or file encryption.

1.1 Purpose of Security Policy

MOREnet's Acceptable Use Policy (AUP) is a companion document to this Security Services Policies document. The Acceptable Use Policy spells out what customers shall and shall not do on the various components of the system, including the type of traffic allowed on the networks. The Security Services Policies internally inform MOREnet staff and managers of the day-to-day implementation of the Acceptable Use Policy in protecting technology and information assets. These two policies also cover incidents when someone outside MOREnet is injured by or interferes with MOREnet-related network activities. Finally, these policies inform MOREnet customers of the mechanisms through which the AUP and Security Services Policies are complied with and enforced.

A. Security Defined: For the purposes of this document, "Security" refers to the integrity of MOREnet owned and/or operated systems, servers and network infrastructure.

B. Acceptable Use Concerns: Some incidents may not involve the integrity of MOREnet owned and/or operated systems, servers, processes and/or network infrastructure. On the other hand, some security incidents may involve non-MOREnet participants. Due to the overlapping areas of concern and the level of expertise required, MOREnet's Security Team is tasked with investigation of both security and AUP concerns. Policies and procedures referred to in this Policy are intended to cover both AUP and Security related incidents.

C. MOREnet's Acceptable Use Policy (AUP), referred to throughout this document, is located at http://www.more.net/about/policies/aup.html.

1.2 Delivery of Security & Acceptable Use Services

MOREnet is committed to certain principles for delivering these services. They include:

A. Confidentiality — Security incidents, consultations or ISREs will be held in strictest confidence by MOREnet staff. Security Incident Reports (SIR) and the resulting responses will not be made available to external organizations unless the customer specifically releases MOREnet to do so or the incident involves MOREnet property interests.

B. Proactive Notification — Security bulletins, advisories or other notifications will be made to MOREnet customers via secure methods to allow them to modify system or network configurations to protect against known security flaws.

C. Accuracy — Security information distributed by MOREnet should be complete, correct and reliable. Incident information will be thoroughly researched and checked by Incident Response Team members before being communicated. Sources of bulletins, advisories and notifications will be screened and clearly identified on distributions from MOREnet to customers.

D. Communication — Interaction among technical contacts at MOREnet customer sites is crucial to a successful security program. MOREnet staff will use secure methods to provide secure communications among customer Security Contacts. PGP is MOREnet's Incident Response Team (IRT)'s standard tool for secure communication with customers, other teams and authorities.

1.3 Availability of Services

MOREnet Security Services are available to all MOREnet customers. Incident response capabilities are part of MOREnet's Reference Desk services under the Membership and Project agreements with a customer. Consulting services are available to all MOREnet customers at the standard hourly rate. ISRE services will be delivered for a fee negotiated between the customer and MOREnet based on the depth and specific customer requirements.

1.4 Designated Contact Persons

MOREnet has identified the need for customer contacts for security matters. This contact will initially default to the Network Coordinator for MERC members, the

Security Coordinator for the Missouri Express project, and the MC1 for CONNECT Project participants. Customers are strongly encouraged to change this contact to reflect the nature of their own local network security practices.

Some MOREnet participants have developed twenty-four hours a day, seven days per week security response teams. This practice is admirable, and should be emulated where possible. MOREnet does not require this capability, but its availability often helps to quickly resolve security incidents without interruption of a network.

1.4.1 Description of Security Contact Role

The person named should bear overall day-to-day responsibility for the network security of the customer. The person should be empowered to act to safeguard the network, and should have access to the expertise to make necessary changes without undue delay. The person need not have the expertise themselves, but should be able to bring appropriate expertise to bear on a problem quickly (i.e., by telephone or pager). The Security Contact need not provide their own email address if the customer has an alternative RFC 2196 recognized emergency contact that is regularly monitored (i.e., abuse@host, hostmaster@host, noc@host, security@host). The alternative address is preferred when available.

The Security Contact need not provide their own telephone number if the customer has developed an alternative regularly monitored telephone point of contact such as a "hot pager" with shared responsibility in a networking group. The alternative telephone number is preferred when available.

The Security Contact should, if possible, be familiar with and have installed PGP or PGPmail for secured communications. On notification that a Security Contact has a

PGP key, MOREnet's Security Team will on verification sign the contact's public key. Instructions for downloading and installing PGP are provided on MOREnet's web site at http://www.more.net/security/.

The Security Contact must be an employee of the customer. No outside consultants are permitted as a Security Contact, to eliminate delays in action or approval. The Security Contact is free to refer technical questions to an outside consultant for technical assistance.

1.4.2 MOREnet Responsibilities to Security Contact

The Security Contact will be MOREnet's preferred point of contact with a customer on security matters. Only in the event a Security Contact is not available or responsive will attempts be made to reach other contacts.

MOREnet will forward relevant notices of security vulnerability and advisories, software bugs affecting security, notices of available security related training and quarterly summaries of security statistics to the Security Contact.

2.0 MOREnet Security Team

2.1 Team Resources

MOREnet has identified internal resources to deliver Security and Acceptable Use investigative services. These resources have been combined into MOREnet's Security Team, a working group of staff who are knowledgeable in areas of supported network operating systems, network servers and network infrastructure (routers, gateways, firewalls, etc.). The Security Team will respond to reported MOREnet security incidents, conduct proactive training sessions and seminars, and provide consulting and ISRE services.

A library of security resources will be created as well as examples of security policies, procedure documents, and other documents beneficial to MOREnet customers concerned with increasing levels of security on their systems and networks. These publications will be updated frequently, and documents made available to MOREnet customers as copyright permits.

MOREnet will maintain software and other resources on the secured ftp server for customer access. Security programs and files will have authentication checks for customer verification of the integrity of the software file. The Security Team will build and maintain a knowledge base gathered from various Internet news groups, publications and peers, and use this resource to deliver the services identified above. Open access to this knowledge base will not be allowed.

2.2 General Team Composition

The MOREnet Security team is responsible for MOREnet's implementation of security measures on internal and shared resources. Specifically, this group's responsibilities include:

A. Coordination of implementation and tracking of MOREnet's security protocols and procedures.

B. Oversight of system and network configuration security of all shared and backbone servers, routers and other devices.

C. Coordination of internal network server and network device configuration security including routing, filtering and other configurations.

D. Coordination of implementation of MOREnet's ongoing Continuous Security Improvement program.

2.3 Security Coordinator

MOREnet has identified a Security Coordinator to administer security services. The Security Coordinator's responsibilities include:

A. Coordination of the Security Team, including:

1. Team composition for resolution of a specific incident

2. Identifying and coordinating training of team members

3. Identifying and coordinating professional development opportunities related to security topics

4. Coordination of response to Security Incident Reports (SIR) from customers and external sources

5. Coordination of ISRE services and negotiation with customers

6. Coordination of security consulting services and negotiation with customers

7. Interacting with external teams and security groups, and law enforcement organizations when appropriate

8. Coordination of security-related training sessions and seminar offerings for customers

9. Maintenance of internal MOREnet protocols and procedures for SIRs and service requests

10. Report to the MOREnet Management Team, Executive Committee and State Projects Steering Committee to review security services provided

3.0 Team Coordination

3.1 Coordination with CERT

MOREnet cooperates with the Computer Emergency Response Team (CERT) located at Carnegie Melon University for reporting and resolution of security incidents.

The CERT Coordination Center is the organization that grew from the computer emergency response team formed by the Defense Advanced Research Projects Agency (DARPA) in November 1988 in response to the needs identified during the "Internet Worm" incident, a malicious program that shut down about 6,000 government and university computers.

The CERT charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts; to take proactive steps to raise the community's awareness of computer security issues; and to conduct research targeted at improving the security of existing systems.

A. MOREnet will regularly report summaries of security reports and resolutions to CERT for inclusion in CERT reports. These reports will include information on all incidents, but include only specific data about the incident(s) which has been authorized for release by the customer reporting. Any reports to CERT, MOREnet committees or other external sources will not identify specific customers, nor will the reports be generated in such a manner that specific customers could be identified unless the customer specifically releases MOREnet to do so.

B. The MOREnet Security Coordinator will create a quarterly summary report of all security incident reports for inclusion in MOREnet reports. This report will not disclose any customer information that may be used to identify the customer.

3.2 Reporting Incidets to Outside Authorities

Reporting of incidents to appropriate authorities is solely at the customer's option, except MOREnet reserves the right to report incidents involving MOREnet property interests. MOREnet will not report incidents or information about other incidents to appropriate authorities unless the customer has specifically released MOREnet to do so.

A. Releases given to MOREnet to permit release of security incident related information can be written, faxed or delivered by e-mail. Such releases must be signed by an authorized individual of the involved institution. In the event of a security incident where the IRT believes e-mail security may have been compromised, a written or fax authorization may be required at the discretion of the Security Manager or Security Coordinator.

B. For incidents when MOREnet does not have a customer release to discuss the information and that do not involve MOREnet property interests, MOREnet will not release, communicate or transfer any information of a specific incident obtained as a result of investigation into that incident without a lawfully executed subpoena or judge's order. Requests from law enforcement or other authorities will be denied without the customer's release or the above legal orders.

C. MOREnet will cooperate fully with all law enforcement or other authorities to investigate and resolve incidents on a customer's behalf. A customer may elect to report the incident to the appropriate authority, and then turn over the incident to MOREnet for coordination with the authority. All contact with and communication between authorities and MOREnet are confidential and may be shared only with appropriate MOREnet staff and the customer.

D. Information disclosed to MOREnet's IRT during the course and scope of an investigation is confidential in nature. Release to other parties will be made only as necessary to resolve an incident, and does not release other parties to disclose that information outside the MOREnet-information recipient relationship.

E. Receipt of a release does not constitute a waiver of any rights held by MOREnet or the University of Missouri to its work product and/or property, and does not guarantee MOREnet will release any such materials.

F. All inquiries regarding requests for information and/or information release shall be directed to MOREnet's Communications Officer, whose public e-mail address is info@more.net. E-mail queries about general public information will be honored, but no request for disclosure of confidential materials outside the course and scope of incident resolution will be honored.

4.0 Security Incident Response

4.1 Incident Response Goals

These goals may be prioritized differently depending on the nature of the incident. Objectives for dealing with incidents include:

A. Figure out how it happened.

B. Find out how to avoid further exploitation of the same vulnerability.

C. Avoid escalation and further incidents.

D. Assess the impact and damage of the incident.

E. Recover from the incident.

F. Update policies and procedures as needed.

G. Find out who did it (if appropriate and possible).

H. Take actions to prevent and/or deter the action from recurring.

I. Document the incident and preserve evidence where possible, for reporting purposes and effective resolution of an incident.

Depending on the nature of the incident, there may be a conflict between analyzing the original source of a problem and restoring systems and services. Overall goals (such as maintaining the operation of critical systems) may supersede the goal of detailed analysis of an incident. It remains the customer's decision, but all involved parties must be aware that without analysis the same incident may happen again.

4.2 Security Incident Response Priorities

Actions to be taken during an incident should be prioritized before an incident occurs. An incident may be so complex that it is impossible to respond to everything at once, so priorities are essential.

An important implication for defining priorities is that once human life and national security considerations have been addressed, it is generally more important to save data than to save system software and hardware. Although it is undesirable to have any damage or loss during an incident, systems can be replaced. However, the loss or compromise of data (especially classified or proprietary data) is usually not an acceptable outcome.

Another important concern is the effect on others, beyond the systems and networks where the incident occurs. Within the limits imposed by government regulations it is always important to inform affected parties as soon as possible. Due to the legal implications, it should be included in planned procedures to avoid delays and uncertainties for administrators.

A. Protect human life and safety; human life always has precedence over all other considerations.

B. Protect classified and/or sensitive data. Prevent exploitation of classified and/or sensitive systems, networks or sites. Inform affected classified and/or sensitive systems, networks or sites about penetrations, bearing in mind local, state and federal laws and regulations.

C. Protect other data, including proprietary, scientific, managerial and other data, because loss of data is costly. Prevent exploitation of other systems, networks or sites and inform affected systems, networks or sites about successful penetrations.

D. Prevent damage to systems (for example, loss or alteration of system files, damage to disk drives, etc.). Damage to systems can result in costly down time and recovery.

E. Minimize disruption of computing resources (including processes). In many cases it is better to shut a system down or disconnect from a network than to risk damage to data or systems. Sites must evaluate the trade-off between shutting down and disconnecting, and staying up. The damage and scope of an incident may be so extensive that the MOREnet infrastructure is compromised and mandates a shutdown.

4.3 Customer Security Incident Response Obligations

All MOREnet customers have an obligation to comply with MOREnet's Security Services Policies. MOREnet Member Representatives are responsible for ensuring organizational compliance, including the customer's responsibility to conduct reasonable investigation on request by the MOREnet Security Coordinator or Manager, report the findings of those investigations within a reasonable time and take reasonable action to cure any breach of the Security Services Policies.

4.4 Security Report Tracking

When a report of an alleged Security incident is received, a MOREnet staff member will immediately enter a tracking report in a secure database or refer the matter to the Reference Desk for initial investigation and creation of a secured tracking report. MOREnet's AUP is located at http://www.more.net/about/policies/aup.html.

4.5 Security Notification

The Security Manager and Security Coordinator are notified of the creation of an Security related tracking report. Should the event occur outside regular office hours, the reporting person will call the security pager.

4.6 Security Incident Response Team Composition

The Security Manager and Security Coordinator will assign team members with appropriate expertise to handle varying stages of each incident, with the Security Coordinator handling coordination of team members and investigation.

4.7 Security Reporting Model

Team members will use the MOREnet Incident Response Form located at http://www.more.net/security/incident/incident.html as a data gathering model.

4.8 Secure Handling of Security Investigative Results

Team members, bearing in mind the need to preserve all relevant logs, communications and other electronic evidence of an alleged Security violation, will place all such electronic notes in a secured database to which only Security Team members have access. Any hardcopy documents, fax communications or other evidence not suitable for storage in this database shall be secured under lock in a location designated by the Security Manager or Coordinator, and a log established to preserve a chain of custody.

4.9 Security Investigation

Team members will establish or disprove the existence of a bona fide AUP or Security incident. Team members, after investigation and based on professional expertise in consultation with other team members, involved institutions and CERT, will recommend action to the involved institution(s)to end the incident or reduce future vulnerability. Team members, within the confines of the MOREnet Product Support matrix, will assist the affected institution(s) in closing the incident or reducing future vulnerability.

4.10 Interim Security Safeguards

Team members may certify to the Security Manager that a present threat exists to other institutions or individuals or institutions outside the affected institution. The Security Manager or Coordinator will inform the appropriate Project Manager(s) of such an occurrence. In such a case, the Security Manager or Coordinator will approve appropriate interim measures to safeguard the interests of affected institutions and inform the appropriate MOREnet Project Manager of those actions.

A. When devising interim safeguards, as time permits, the Security Manager or Coordinator will consult the appropriate MOREnet Project Manager(s)for appropriate interim measures.

B. Interim measures will balance least intrusive alternatives against the nature and severity of security breaches, and may include blocking a site's network traffic at the MOREnet hub router in exigent circumstances.

4.11 Security Incident Closure

Team members will report the end of an incident to the Security Coordinator, who will request an incident letter from the appropriate institution(s). The incident letter must be hardcopy and signed by an authorized individual of the appropriate institution. The incident letter must be received by MOREnet Security within ten (10) working days of request. If the letter is not received within that time, a second request will be made, and the letter must be received within five (5) working days of the second request. If no letter is received within five (5) working days of the second request, the Security Manager or Coordinator may escalate the incident to the appropriate Project Manger for disciplinary purposes. This letter, at minimum, must include:

A. Date and nature of the incident's initiation.

B. Names of institutions involved.

C. Nature of the incident, including the nature of exploitation where applicable.

D. Date of incident's closure.

E. How the incident was resolved.

F. General nature of any disciplinary actions taken.

G. Type and nature of actions taken to end the incident or reduce future vulnerability to this type of exploitation.

4.12 Security Safeguards in Event of Noncompliance

In the event a MOREnet customer does not respond within a reasonable time to Security Team requests, is uncooperative or declines to ease or remedy an established Security violation, the Security Manager or Coordinator will take interim, non-disciplinary measures to safeguard the interests of affected institutions as discussed above and inform the appropriate MOREnet Project Manager of those actions. The Security Manager or Coordinator will then send a certified letter, return receipt requested, to the unresponsive institution. If there is no response or the incident/vulnerability continues unabated for five (5) working days after receipt of the letter, the Security Manager or Coordinator refer the incident to the appropriate Project Manager for disciplinary action while maintaining interim safeguards.

5.0 Acceptable Use Policy Incident Response

5.1 AUP Incident Response Goals

These goals may be prioritized differently depending on the nature of the incident. Objectives for dealing with incidents include:

A. Figure out how it happened.

B. Find out how to deter or prevent the action from recurring.

C. Avoid escalation and further incidents.

D. Assess the impact and damage of the incident.

E. Bring the parties back into compliance with the AUP.

F. Update policies and procedures as needed.

G. Find out who did it (if appropriate and possible).

H. Take actions to prevent and/or deter the action from recurring.

I. Document the incident and preserve evidence where possible, for reporting purposes and effective resolution of an incident.

Depending on the nature of the incident, there may be a conflict between analyzing the original source of a problem and restoring systems and services. Overall goals (such as maintaining the operation of critical systems) may supersede the goal of detailed analysis of an incident. It remains the customer's decision, but all involved parties must be aware that without analysis the same incident may happen again.

5.2 AUP Incident Response Priorities

Actions to be taken during an incident should be prioritized before an incident occurs. An incident may be so complex that it is impossible to respond to everything at once, so priorities are essential.

An important implication for defining priorities is that once human life and national security considerations have been addressed, it is generally more important to save data than to save system software and hardware. Although it is undesirable to have any damage or loss during an incident, systems can be replaced. However, the loss or compromise of data (especially classified or proprietary data) is usually not an acceptable outcome.

Another important concern is the effect on others, beyond the systems and networks where the incident occurs. Within the limits imposed by government regulations it is always important to inform affected parties as soon as possible. Due to the legal implications, it should be included in planned procedures to avoid delays and uncertainties for administrators.

A. Protect human life and safety; human life always has precedence over all other considerations.

B. Protect classified and/or sensitive data. Prevent exploitation of classified and/or sensitive systems, networks or sites. Inform affected classified and/or sensitive systems, networks or sites about penetrations, bearing in mind local, state and federal laws and regulations.

C. Protect other data, including proprietary, scientific, managerial and other data, because loss of data is costly. Prevent exploitation of other systems, networks or sites and inform affected systems, networks or sites about successful penetrations.

D. Prevent damage to systems (for example, loss or alteration of system files, damage to disk drives, etc.). Damage to systems can result in costly down time and recovery.

E. Minimize disruption of computing resources (including processes). In many cases it is better to shut a system down or disconnect from a network than to risk damage to data or systems. Sites must evaluate the trade-off between shutting down and disconnecting, and staying up. The damage and scope of an incident may be so extensive that the MOREnet infrastructure is compromised and mandates a shutdown.

5.3 Customer AUP Incident Response Obligations

All MOREnet customers have an obligation to comply with MOREnet's Acceptable Use Policy. MOREnet Member Representatives are responsible for ensuring organizational compliance, including the customer's responsibility to conduct reasonable investigation on request by the MOREnet Security Coordinator or Manager, report the findings of those investigations within a reasonable time and take reasonable action to cure any breach of the Security Services Policies.

5.4 AUP Report Tracking

When a report of an alleged Acceptable Use Policy (AUP) violation is made to MOREnet, a MOREnet staff member will immediately enter a tracking report in a secure database or refer the matter to the Reference Desk for initial investigation and creation of a secured tracking report. MOREnet's AUP is located at http://www.more.net/about/policies/aup.html.

5.5 AUP Notification

The Security Manager and Security Coordinator are notified of the creation of an AUP related tracking report. Should the event occur outside regular office hours, the reporting person will call the security pager.

5.6 AUP Incident Response Team Composition

The Security Manager and Security Coordinator will assign team members with appropriate expertise to handle varying stages of each incident, with the Security Coordinator handling coordination of team members and investigation.

5.7 AUP Reporting Model

Team members will use the MOREnet Incident Response Form at http://www.more.net/security/incident/incident.html as a data gathering model.

5.8 Secure Handling of AUP Investigative Results

Team members, bearing in mind the need to preserve all relevant logs, communications and other electronic evidence of an alleged AUP violation, will place all such electronic notes in a secured database to which only Security Team members have access. Any hardcopy documents, fax communications or other evidence not suitable for storage in this database shall be secured under lock in a location designated by the Security Manager or Coordinator, and a log established to preserve a chain of custody.

5.9 AUP Investigation

Team members will establish or disprove the existence of a bona fide AUP incident. Team members, after investigation and based on professional expertise in consultation with other team members, involved institutions and CERT, will recommend action to the involved institution(s) to end the incident or reduce future vulnerability.

Team members, within the confines of the MOREnet Product Support matrix, will assist the affected institution(s)in closing the incident or reducing future vulnerability.

5.10 Interim Acceptable Use Safeguards

Team members may certify to the Security Manager that a present threat exists to other institutions or individuals or institutions outside the affected institution. The Security Manager or Coordinator will inform the appropriate Project Manager(s) of such an occurrence. In such a case, the Security Manager or Coordinator will approve appropriate interim measures to safeguard the interests of affected institutions and inform the appropriate MOREnet Project Manager of those actions.

A. When devising interim safeguards, as time permits, the Security Manager or Coordinator will consult the appropriate MOREnet Project Manager(s)for appropriate interim measures.

B. Interim measures will balance least intrusive alternatives against the nature and severity of Acceptable Use Policy breaches, and may include blocking a site's network traffic at the MOREnet hub router in exigent circumstances.

5.11 Acceptable Use Policy Incident Closure

Team members will report the end of an incident to the Security Coordinator, who will request an incident letter from the appropriate institution(s). The incident letter must be hardcopy and signed by an authorized individual of the appropriate institution. The incident letter must be received by MOREnet Security within ten (10) working days of request. If the letter is not received within that time, a second request will be made, and the letter must be received within five (5) working days of the second request. If no letter is received within five (5) working days of the second request, the Security Manager or

Coordinator may escalate the incident to the appropriate Project Manger for disciplinary purposes. This letter, at minimum, must include:

A. Date and nature of the incident's initiation.

B. Names of institutions involved.

C. Nature of the incident, including the nature of exploitation where applicable.

D. Date of incident's closure.

E. How the incident was resolved.

F. General nature of any disciplinary actions taken.

G. Type and nature of actions taken to end the incident or reduce future vulnerability to this type of incident.

5.12 Safeguards in Event of AUP Noncompliance

In the event a MOREnet customer does not respond within a reasonable time to Security Team requests, is uncooperative or declines to ease or remedy an established AUP violation, the Security Manager or Coordinator will take interim, non-disciplinary measures to safeguard the interests of affected institutions as discussed above and inform the appropriate MOREnet Project Manager of those actions. The Security Manager or Coordinator will then send a certified letter, return receipt requested, to the unresponsive institution. If there is no response or the incident/vulnerability continues unabated for five (5) working days after receipt of the letter, the Security Manager or Coordinator refer the incident to the appropriate Project Manager for disciplinary action while maintaining interim safeguards.

MOREnet Security Practices

Document Status

This document describes current MOREnet practices in implementing these existing policies:

A. MOREnet Acceptable Use Policy:

http://www.more.net/about/policies/aup.html

B. MOREnet Security and Use Policy:

http://www.more.net/security/materials/secpol.html

The current version of this document is maintained at http://www.more.net/security/materials/practices.

Nothing in this document signifies any change in the way MOREnet does business. This practice document simply documents MOREnet Security event handling methodology and implementation as practiced over the last five years.

If you have questions about this MOREnet Security Practices document, its interpretation or enforcement, please e-mail security@more.net.

Philosophy

MOREnet currently manages over 1,100 edge routers at customer sites, and provides security services to each site. MOREnet customer contracts are for bandwidth; there is no funding, staffing or provision for local firewalls, proxy servers, intrusion detection or other traditionally local security measures.

MOREnet uses several tools to provide security services to customers, and support the MOREnet Acceptable Use Policy. These defensive measures include Access Control Lists and scanning.

Access Control Lists

Access Control Lists (ACLs) are a feature in many router and server operating systems. ACLs can examine each network packet, by source, destination, ports in use and protocol. They are a valid tool for network defense. However, ACLs slow down routing because as they consume processor time. MOREnet does not use ACLs in devices that MOREnet manages for this reason.

MOREnet expressly reserves the right to implement ACLs in any MOREnet managed edge devices during an immediate security event to protect MOREnet, the MOREnet network, other MOREnet customers and outside networks.

Support of Access Control Lists for Customers

MOREnet provides informational support on router ACLs for customers. MOREnet does not provide ACLs for customers to enforce local policies.

Scanning

Scanning refers to a series of messages sent over the Internet, each associated with a "well-known" port number that a computer provides. The response received indicates whether the port is used and frequently returns information on a system's software and version. Scanning involves collection of information that can be viewed by any Internet connection.

MOREnet Security staff may, on reasonable suspicion of a threat to the shared network, defensively scan without notice to make an initial risk assessment and/or confirm a reported potential breach of the Acceptable Use Policy. These scans may be of a single customer machine or an entire customer network, based on the risk to the shared network.

Scope and Duration of Defensive Measures

MOREnet will tailor any defensive measures taken to defend against a specific problem. Reasonable efforts will be made to work with an organization in order to limit impact of any ACL. It should be noted, however, that in networks without IP accountability, any blocking may have a greater impact than a single computer.

MOREnet-employed defensive measures will also be limited in time to that which is reasonably necessary to remove an active threat from the network, but may be extended at MOREnet's discretion when MOREnet Security certifies the customer is making good faith efforts to restore accountability and risk mitigation.

The MOREnet Acceptable Use Policy requires customers to "make reasonable efforts to ...ensure compliance of those connected through them." MOREnet reserves the right to continue any block where there is a failure to provide accountability, pending review by the MOREnet Executive Director. Networks and devices that are not accountable cannot ensure compliance.

Immediate Security Events Defined

The following are established "immediate security events."

A. Attacks in progress

B. Denial of service conditions

C. Compromise of accountability

This list is not exhaustive. Technologies change and as new exploits are discovered, this list is likely to be modified.

The following events are not "immediate security events."

A. Unauthorized port scanning, network scanning, banner grabbing and other forms of reconnaissance. While these activities are commonly viewed as reconnaissance prior to

6. Where a site has been repeatedly advised of lack of accountability and has failed to make reasonable efforts to provide accountability, future similar violations will be handled as organizational breaches of the MOREnet Acceptable Use Policy. MOREnet may, at its discretion, continue any reasonably necessary defensive measures pending resolution of that complaint.

REFERENCES

Aeilts, T. (January, 2005). Defending against cyber crime and terrorism: a new role for universities. The FBI Law Enforcement Bulletin.

Attorney General. (August, 1999). 1999 Report on cyberstalking: A new challenge for law enforcement and industry. A report from the Attorney General to the Vice President. Washington, DC.

Bouffard, M. (1998). A Commercially Viable Computer Security Implementation Framework. Unpublished master's thesis. Montreal: Concordia University.

Bruhn, M. & Petersen, R. (2003). Planning for improved security. Educause Review, 38 (6), 98.

Busch, C., De Maret, P.S., Flynn, T., Kellum, R., Meyers, S., Saunders, M., White, R., & Palmquist, R. (2005). Content Analysis. Writing@CSU. Retrieved [Date] from Colorado State University, Department of English Web site: http://writing.colostate.edu/guides/research/content/

Carlson, S. (2003). Cal poly campus faces battle over proposed anti-pornography resolution. Chronicle of Higher Education, 49(27), A31.

Culpepper, L. & Santana, R. (2000). Computer policies at Louisiana-Monroe rely heavily on trust. Black Issues in Higher Education, 16 (25), 38.

Davis, Z. (2005). Computer Desktop Encyclopedia. PCMAg.com. Point Pleasant, PA: The Computer Language Company Inc.

Eisler, D. L. (2001). Higher education communication and information systems policy. New Directions for Higher Education, 115, 71.

Etheir, M. (1997). Colleges adopt a range of policies to regulate use of campus networks. Chronicle of Higher Education, 43 (48), A21.

Fitzer, K., Griffin, K., Kastor, G., & Kelsey, Y. (2002). Computer Hacking. Urbana-Champaign, IL: University of Illinois.
This white paper was created by four graduate students in the Curriculum, Technology, and Education Reform (CTER) Masters of Education program at the University of Illinois at Urbana-Champaign.

Harrison. D. L. The Patriot Act: A new way of thinking. Higher education issues after the USA Patriot Act. Division of Legal Affairs. Office of the President: The University of North Dakota. Retrieved March 20, 2006, from the NACUA Web site: www.nacua.org/documents/PatriotAct_Outline.pdf

Leedy, P & Ormrod, J. (2004). Practical Research: planning and design. Upper Saddle River, NJ: Merrill Prentice Hall.

Luker, M. (1998). Net@EDU focuses on academic networking. Educom Review, 33 (6) 60.

Lorch, M. (2004). PRIMA—Privilege Management and Authorization in Grid Computing Environments. Unpublished doctoral dissertation. Blacksburg, VA: Virginia Polytechnic Institute and State University.

McCollum, K. (1998). With computer hacking on the rise, colleges seek ways to handle attacks. Chronicle of Higher Education, 44 (35), A27.

McGinnis and Comstock (2003). The Implications of Information Assurance and Security Crisis on Computing Model Curricula. Information Systems Education Journal, 1 (9).

Mitrano, T. (2004). How Colleges Should Respond to File-Sharing Charges. Chronicle of Higher Education, 50 (42), B16.

Nevada grapples with computer policy. (1998, December). Community College Week. 11(11). 16.

North Dakota University System Policies (2005). NDUS Procedures. Retrieved March 25, 2006, from the North Dakota University System Web site: http://www.ndus.edu/policies/ndus-policies/subpolicy.asp?ref=2551

Oblinger, D & Petersen, R. (2004). Cyber security: It takes a community. University Business, 7 (4), 88.

O'Neil, R. (2003). What limits should campus networks place on pornography? Chronicle of Higher Education, 49 (28), B20.

Petersen, R. J. (2002). What's policy got to do with IT? Educause Review, 37 (2), 52.

Petersen, R. (2004, April). Protecting our nation's cyber space: educational awareness for the cyber citizen. Testimony and statement for the record before the subcommittee on technology, information policy, intergovernmental relations and the census committee on government reform. Washington, DC: House of Representatives.

Petersen, R. (2004). Efforts to increase cyber security on campuses in an era of shrinking budgets. Chronicle of Higher Education, 50 (41), B4.

Petersen, R. (2005) Security Breaches: Notification, treatment and prevention. Educause Review, 40 (2), 78.

Reid, I. C. (2001). Knowledge: how should universities manage IT? Perspectives: Policy & Practice in Higher Education, 5 (1), 21.

Selingo, J. (1997). Colleges step up efforts to teach students about computer-security issues. Chronicle of Higher Education, 44 (5), A28.

Sern, G. (2000). Crises and collaboration in the new millennium. Educause Review, 35 (6), 92.

The Missouri Research and Education Network (MOREnet) (2005). Policies and Procedures. Retrieved February 15, 2006, from the MOREnet Web site: http://www.more.net/about/policies/index.html

Van Trieste, R. (2001). Basic Computer Terms for PCs. Internet.

Wikipedia. (2005). GNU Free Documentation License. Retrieved January 3, 2006, from http://en.wikipedia.org/wiki/Wikipedia:Text_of_the_GNU_Free_Documentation_License

Wilson, D. L. (1994). Threats to internet security. Chronicle of Higher Education, 40 (30), A22.

Wilson, D. (1994). Convenience vs. security on the internet. Chronicle of Higher Education, 40 (45), A15.

WordNet 2.0. (2003). A lexical database for the English language. Retrieved December 15, 2005, from Princeton University, Cognitive Science Laboratory Web site: http://wordnet.princeton.edu/

Young, J. R. (1998). Techno-realists hope to enrich debate over policy issues in cyberspace. Chronicle of Higher Education, 44 (30), A23.