1-1-2005

Computer Security Perceptions Of Students Attending The School Of Technology At Eastern Illinois University

David C. Fulton
Eastern Illinois University

THESIS REPRODUCTION CERTIFICATE

'O: Graduate Degree Candidates (who have written formal theses)

;UBJECT: Permission to Reproduce Theses

he University Library is receiving a number of request from other institutions asking permission to reproduce dissertations for ıclusion in their library holdings. Although no copyright laws are involved, we feel that professional courtesy demands that ermission be obtained from the author before we allow these to be copied.

'LEASE SIGN ONE OF THE FOLLOWING STATEMENTS:

looth Library of Eastern Illinois University has my permission to lend my thesis to a reputable college or university for the purpose of opying it for inclusion in that institution's library or research holdings.

Author's Signature

12/13/05

Date

respectfully request Booth Library of Eastern Illinois University **NOT** allow my thesis to be reproduced because:

_____

_____

_____

_____ _____

Author's Signature

Date

This form must be submitted in duplicate.

Computer Security Perceptions of Students Attending the

School of Technology at Eastern Illinois University

(TITLE)

BY

David C. Fulton

THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF

Master of Science in Technology

IN THE GRADUATE SCHOOL, EASTERN ILLINOIS UNIVERSITY
CHARLESTON, ILLINOIS

2005

YEAR

I HEREBY RECOMMEND THAT THIS THESIS BE ACCEPTED AS FULFILLING
THIS PART OF THE GRADUATE DEGREE CITED ABOVE

12/13/2005
DATE

Samuel Guccione
THESIS DIRECTOR

12-13-05
DATE

DEPARTMENT/SCHOOL HEAD

THESIS COMMITTEE

Sam Guccione

12/13/05

Sam Guccione, Ed.D, C.S.I.T.
Professor
Thesis Director
School of Technology

Date

L C Butler

12-13-05

Louis C. Butler, Ph.D.
Professor
School of Technology

Date

Peter P. Liu

12/13/05

Peter Ping Liu
Ph.D., P.E., OCP, C.Q.E., and C.S.I.T.
Professor
Graduate Coordinator
School of Technology

Date

Running head: COMPUTER SECURITY PERCEPTIONS OF STUDENTS ATTENDING

Computer Security Perceptions of Students Attending the School of Technology at Eastern Illinois University

David C Fulton

Eastern Illinois University

Abstract

Computer security is a major concern that demands attention. Computer viruses and other security risks proliferate on a daily basis. In the academic environment several disciplines of learning may share a common network or computer environment. This situation presents a number of challenges for a university. Allowing access to the Internet yet protecting the interests of the school can be a difficult undertaking. Data protection and the liabilities associated with protecting data is a major undertaking for a university.

This thesis examines the perceptions of students attending the School of Technology at Eastern Illinois University in the area of computer security. Use of hardware and software are a substantial means of protection. However, end user behavior is also an intertwined facet of computer security. For a student to effectively pursue an education usually requires research on the Internet. This thesis further examines what resources the student attending the School of Technology has available in hardware and software. The availability is just the first step for a student to have a secure computer. Providing direction and education about using what is available is also a critical aspect of security.

This work sought to identify the perceptions of a group of those that use the network at Easter Illinois University. A survey was presented to ten classes within the School of Technology at Eastern Illinois University. The results of this survey indicated a general understanding or threats posed by computer malware. The results also indicated specific use of certain software and hardware features in regard to security beyond the initial anti-virus software may need further development.

Acknowledgements

I would like to take this opportunity to express my gratitude to everyone that has assisted me and offered encouragement during my journey through my academic career. Especially involved have been my wife Susie and my family. I want to extend a special thank you for their support and understanding during all the weekends and long evenings of study, research, and preparation for classes.

There have been many that have had an important part in my reaching the point of writing this thesis.

I would like to thank Eastern Illinois University and especially the School of Continuing Education. This school reaches out to the adult student and is very helpful in policies and schedules. Without the efforts of Eastern Illinois University in working with the adult learner this work would not have been possible.

I would also like to thank the School of Technology and those that participated in the survey which provided the data for this body of research. To those Professors and students that helped in this research a special thank you!

I want to thank my thesis committee: Dr. Sam Guccione, Dr. Ping Liu, and Dr. Louis Butler. Each of these Professors played a role in my education. I learned about Total Quality Systems from Dr. Liu and Training Systems Management from Dr. Butler. Dr. Guccione taught the Global Technology class where I first considered the thesis option. Dr. Guccione offered the idea that the thesis option presented a unique opportunity to learn and experience the process in case we ever decided to pursue a Doctorate Degree. Dr Guccione as my thesis director has been very helpful and encouraging during this process and has offered ideas and concepts that have produced this thesis. Thank You Dr. Guccione.

A special thanks also goes to everyone I worked with on projects and team assignments. Some of whom opened my eyes to new ways of doing things and others that simply encouraged me.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

Technology and the use of computers, once only a tool for large businesses employing very technically skilled workers, is today widespread and is used by persons with varied levels of technical abilities. Transactions from small purchases to large financial exchanges occur every minute of every day. The Internet has become a vital means of communication and an essential business tool.

The benefits of technology seem endless. However, these benefits come with a cost. Viruses, Worms, Trojans, Spyware, Adware, Dialers, Spam, Backdoor Access, and intrusion detection are but a few of the security risks anyone using this technology must face. The risks in many cases do not require being connected to the Internet for a problem to occur. The cost linked to these risks total in the billions of dollars each year. Beyond the monetary costs, the implications of identity theft and plagiarism are staggering.

Universities throughout the country use technology in the classroom. Students use technology to communicate with their professors and perform research. Professors, researchers, and students all make use of current technology to perform their tasks. Professors use the Internet to deliver assignments and enhance their classroom instruction. Researchers seek information from around the world to enhance their study and collaborate with researchers across the globe. Students enrich their minds and broaden their horizons through technology and the Internet.

Further, universities are faced with the daunting task of enabling their faculty and students to pursue knowledge and yet maintain a measure of security. During recent years a number of universities faced intrusions of their computer networks. Universities maintain databases of confidential information about their students. This creates many legal responsibilities for

universities. The expense of the associated legal requirements can place a financial burden on a university.

A student entering a university setting is usually making a major lifestyle change. In many cases this may be the first time they have been responsible for a computer of their own. Students may know of viruses or other security issues, but may not be aware of the true nature of the potential for damage. Many students may assume that the university has taken care of all security requirements.

Universities currently face the challenge of informing the student of dangers that exist when technology is used and especially when connected to the Internet. Security enforcement is standard practice in the corporate world. The increasingly destructive nature of current risks now requires that security policies must be established and enforced by universities.

Incoming students need to be able to adequately protect their computers and data. Some universities are currently providing software and instructions on the use of the software to assist new students. Antivirus software alone may not be enough to secure a computer. Many universities place student housing behind firewalls, adding a layer of protection. Students face an array of alternatives and must make choices of which services best suit their needs.

New threats are encountered on a continuing basis as viruses and worms proliferate. Hackers, which in some cases may be fellow classmates, can wreak havoc on computers. These realities, along with daily classroom work, must be dealt with by all students.

Universities have an obligation to assist students with maintaining secure computers. Some universities currently enforce security policies that have been established from previous experience. Further policies may currently be in the process of being drafted and may be

implemented in the future. These policies will be designed to assist the student in maintaining a secure computer.

Eastern Illinois University is no exception from any of these challenges or threats. Specifically considering the SOT (School of Technology) at Eastern Illinois University many of these same challenges are present. Eastern Illinois University takes a proactive stance in establishing computer security policy and taking measures to enforce the policy. Eastern Illinois University makes available a wireless network within their campus area as well as Internet access. By doing so the University provides needed tools for education and research, and by doing so, they expose their network to possible threats.

1.1 Statement of the problem

Universities are placed in a unique position since the risks associated with technology and the Internet is heightened because of the mission of a university. Seeking knowledge requires the use of the Internet, thus the risks are also present. Universities often find themselves vulnerable to security risks when accessing the Internet. As a result, more viruses proliferate in a university setting than a tightly secured network. Universities have become increasingly aware of the problem and have begun to take steps to correct the problem.

Students are usually aware that viruses can cause damage or be an annoyance. The reality of the situation is much grimmer; a worm may expose the students' records, financial and otherwise to an unscrupulous hacker. These same students in most cases may not know how to prevent an infection of their computer or how to eliminate the virus if one is found on their computer. Incoming students may be experiencing an entirely new life style, and securing their computers could be low on their list of priorities.

Universities face a growing problem in educating students about the risks that occur each time they turn on their computer. In years past many universities left this task to a usually overwhelmed IT (Information Technology) department. Educational institutions need to perform risk analyses on student infections similar to those that fiscally responsible businesses in the corporate world perform. Based on this risk assessment a plan should be established to reduce the risk to students and the university. The creation and enactment of this plan is the problem.

Eastern Illinois University has taken steps over the past year to help combat some of these problems. One of the problems was an excessive amount of computer viruses which led to installing software to help control this problem. Note the following statement from an Eastern Illinois University Website:

> For those of you who were here last year, you remember the onslaught of viruses and worms that necessitated interruptions to network services. Starting in the fall of 2005, Network Services is taking a big step towards substantially reducing the effect of viruses and worms on our network. To protect student computers, and ultimately the network we all share, we have installed a new network admissions system called "Clean Access." Clean Access encompasses a new network system installed during the summer. It is used in conjunction with a new software application at the desktop called the "Clean Access Agent," which ensures that all those logging into the network have sufficient virus protection and system updates installed (Eastern Illinois University, 2005)

The information technology department has also added hardware to assist in the control of excessive, unwanted email, commonly called spam.

1.2 Statement of the purpose

The purpose of this study is to identify the perceptions of students attending the School of

Technology at Eastern Illinois University regarding computer security. Students may not be aware of the problems associated with an inadequately secured computer. Further students may not be fully aware of tools available and steps to take as a user to protect their computers. Based on the student perceptions this study may be able to assist Eastern Illinois University officials in determining if further measures are needed to provide a secure environment for students.

1.3 Research Question

Do SOT (School of Technology) Students at Eastern Illinois University have a limited understanding of the risks associated with the use of computers and the Internet? SOT Students at Eastern Illinois University may be unaware or may fail to avail themselves of technologies which may include hardware and software available at Eastern Illinois University to reduce exposure to the risks of current technologies.

1.4 Definition of terms

Hackers: A person that engages in one or more of the following activities: breaking into a private network or private computer is breaking something, such as a network or part of a network, such as a web server, stealing data such as schematics or other valuable information (Maggiora & Doherty, 2003, p. 85).

Malware: A software program designed to fulfill any purpose contrary to the interests of the person running it. Examples of malware include viruses and Trojan Horses

Viruses and Worms: "Viruses and worms are self-replicating programs or code fragments that attach themselves to other programs (viruses) or machines (worms). Both viruses and worms attempt to shut down networks by flooding them with massive amounts of bogus traffic, usually through email" (Maggiora & Doherty, 2003, p. 86).

Trojan Horses: "Trojan horses, which are attached to other programs, are the leading causes of all break-ins, when a user downloads and activates a Trojan horse, the hacked software (SW) kicks off a virus, password gobbler, or remote-control SW that gives the hacker control of the PC" (Maggiora & Doherty, 2003, p. 86).

Firewall: "Firewalls keep both corporate and personal networks safe from attack by inspecting packet for known attack profiles and by acting as a proxy between you and the rest of the world" (Maggiora & Doherty, 2003, p. 95).

Bot: A bot is common parlance on the Internet for a software program that is a software agent. A Bot interacts with other network services intended for people as if it were a real person. One typical use of bots is to gather information. The term is derived from the word "robot", reflecting the autonomous character in the "virtual robot"-ness of the concept (Wikipedia,).

WebCT & Blackboard: E-learning software designed for educational institutions.

SSL (Secure Socket Layers): A security protocol used to secure Web-based communications. The protocol is most often used to secure financial transactions (shopping, banking, etc.), but can be used to secure any TCP/IP-transactions. SSL technology encrypts messages before they are sent so they cannot be read if intercepted. When the messages are received, SSL decrypts them.

1.5 Assumptions

For this study it is assumed that a new virus or worm had not recently made it into Eastern Illinois University's network that would skew the results of the survey.

It is further assumed that the respondents are aware whether or not the problems which they may experience with a computer are an infection or security breach.

1.6 Limitations

Limitations to this study include data accuracy which is dependent upon the respondents' answers to the survey accurately reflecting their perceptions.

A further limitation is that the technology in regard to security is in constant change and respondents may not be aware of the latest changes applied by Eastern Illinois University.

1.7 Delimitations

This study is delimited to the School of Technology at Eastern Illinois University.

Chapter 2

Related Literature

The battle between those that use computers for business, research, and for other everyday uses and those that want to steal, infect, and intrude is in full force. Advancements in computer security occur daily however there seems to be an equally advanced security risk for each new security measure.

2.1 Security Concerns

The business world has found that in regard to security risk the first place of concern is within the organization. Research in the area of end user security behaviors reveals interesting statistics. One such forum of research stated:

> By collapsing across the many similarities among these expert-generated categories, we developed a six element taxonomy of security behavior that varied along two dimensions: intentionality and technical expertise. The intentionality dimension appeared to capture whether the behavior described was intentionally malicious, intentionally beneficial, or perhaps somewhere in between (i.e., absent explicit intention to help or harm). The technical expertise dimension focused on the degree of computer or information technology knowledge and skill that the actor needed to have in order to perform the behavior described on the card (Stanton, Stam, Mastrangelo &, Jolton, 2005, p. 126).

(Stanton et al, 2005, p. 126) developed the following table illustrating the two dimensions and categories this research examined.

Table 2-1 Two factor taxonomy of security behaviors

Expertise	Intentions	Title	Description
High	Malicious	Intentional Destruction	Behavior requires technical expertise together with a strong intention to do harm to the organization's IT and resources. Example: employee breaks into an employer's protected files in order to steal a trade secret. 2
Low	Malicious	Detrimental Misuse	Behavior requires minimal technical expertise but nonetheless includes intention to do harm through annoyance, harassment, rule breaking, etc. Example: using company email for SPAM messages marketing a sideline business.
High	Neutral	Dangerous Tinkering	Behavior requires technical expertise but no clear intention to do harm to the organization's IT and resources. Example: employee configures a wireless gateway that inadvertently allows wireless access to the company's network by people in passing cars.
Low	Neutral	Naïve Mistakes	Behavior requires minimal technical expertise and no clear intention to do harm to the organization's information technology and resources. Example: choosing a bad password such as "password."
High	Beneficial	Aware Assurance	Behavior requires technical expertise

				together with a strong intention to do good by preserving and protecting the organization's information technology and resources. Example: recognizing the presence of a backdoor program through careful observations of own PC.
Low	Beneficial	Basic		
			Hygiene	Behavior requires no technical expertise but includes clear intention to preserve and protect the organization's IT and resources. Example: a trained and aware employee resists an attempt at social engineering by refusing to reveal her password to a caller claiming to be from computer services.

One interesting concept which may escape notice is that even an intrusion which is not meant to harm is still a security risk. Information security includes keeping data secure and confidential.

With information on disks that could potentially be accessed from a remote location there has been a proliferation of security issues. Among the concerns are viruses, worms, denial of service attacks, and data theft. These concerns have led to an entire industry dedicated to combating those that seek to illegally access information or damage computer networks. The industry of information security has developed software and hardware designed to protect your information and hardware.

In 1981 Cohen became interested in a virus that would attach itself to other programs and subsequently gain control of the infected computer. Cohen developed such a virus and eventually received permission to test the virus on a UNIX computer at the University of Southern California. The virus was very effective, gaining full administrative rights to the system in each of the five tries. It never took the virus more than an hour to gain these rights and in one case only took five minutes (Hayes, 2003, p. 26).

Viruses have been a threat to security ever since Cohen's research. Initially the defenses against such viruses were mostly ad hoc, being used after an attack. Eventually virus and intrusion software were developed. Then in 1991 Eugene Spafford at the University of Purdue introduced the term; firewall (Hayes, 2003, p. 26). Other areas of security were developed during the 1990's, including Secure Sockets Layer (SSL) and automatic encryption and authentication to TCP/IP (Hayes, p. 26).

The threats will continue from hackers. Technology continues to grow with new devices and technology available and more people are availing themselves of the available technologies. Software vendors have recognized the threats and have sought to improve the weaknesses in their software. More devices are being equipped with firewall and antivirus software as part of the device package. New areas have been exposed for potential threats including E-Business and those that employ the use of wireless services (Hulme, 2004, p. 67).

Effort on the part of an end user is required and education of the end user is essential. Security options that are hidden or buried several menus deep loose their effectiveness. (Furnell, 2005) commenting on a collaborative survey conducted by America Online and the National Cyber Security Alliance of domestic Internet users in the United States notes the following:

> Based upon a sample of 329 homes (59% using broadband access and 41% using dial-up connections) the study determined a number of worrying findings. For example, more than half of the respondents were not clear on the difference between anti-virus and firewall protection. Moreover, many of them were not using the technologies effectively – a scan of the respondents' systems revealed that 67% either had no anti-virus software on their system at all or had not updated it within the previous week and 72% lacked a properly configured firewall (Furnell, 2005, p. 275).

In view of these findings it is evident that a majority of end users either lack the technical understanding or the presentation of the available measures for protection is not present. Some recent developments may help change this situation. (Furnell, 2005) further notes:

> From the perspective of protecting the average user there has been some notable progress in the last year, with developments such as Windows XP Service Pack 2 and its concentration of the OS-level features within the Security Center (for dealing with firewall, automatic updates, and virus protection), and the default enabling of features such as the Windows Firewall (Furnell, 2005, p. 275).

Making the security measures available and in one location will certainly help the average end user become more aware of security measures such as anti-virus software or a firewall that may have been disabled either by a user or another program. This awareness is one of the first steps to maintaining a secure computer.

Yet another area of security concerns is that of data security. A recent security breach may have exposed up to 40 million credit cards. (Krazit, 2005) reporting on this breach stated:

> A hacker was able to access potentially 40 million credit card numbers by infiltrating the network of a company that processed payment data for MasterCard International Inc. and

other companies, MasterCard said Friday. MasterCard has notified banks that issue its credit cards about the security breach, which victimized CardSystems Solutions Inc., a Tucson, Ariz. back-office processing company, said Jessica Antle, a MasterCard spokeswoman. Those banks will then take steps to notify their customers as they see fit, she said. The network at CardSystems had certain vulnerabilities that allowed an outsider to access the card numbers, 13.9 million of which were connected to MasterCard cards, Antle said. MasterCard's fraud detection system first became aware of the infiltration in May, and the company promptly launched an investigation into the breach... Companies such as CardSystems process payment data for multiple credit card companies, which is why MasterCard numbers only accounted for 13.9 million of the numbers, Antle said... Security breaches don't always happen through hacking into a company's network. Citigroup Inc. recently notified customers that the credit information of 3.9 million customers was inside a package that disappeared while in transit from New Jersey to Texas in the care of United Parcel Service Inc. (Krazit, 2005, p. 1)

Data security is a major concern in the business world. Identity theft is a major problem affecting society, so breaches such as the one at Card Systems Inc. are a security issue that must be rectified. One measure that is being established is the Payment Card Industry (PCI) data security standard. (Vijayan, 2005) comments on standards being pushed:

The Payment Card Industry (PCI) data security standard being pushed by MasterCard International Inc. and Visa U.S.A. Inc. went into effect today for all merchants handling credit card data, but concerns remain about its implementation and compliance validation. Under PCI, all companies that accept credit cards are required to comply with 12 security-related requirements that call for, among other things, encrypted transmission of cardholder

data, periodic network scans, logical and physical access controls, activity monitoring and logging (Vijayan, 2005).

Certain security standards are being set for this industry. However, it seems that industry is able to decide what measures need to be taken.

Further emphasizing the danger that a compromised computer can present is documented by (Grimes, 2005):

> What was once the domain of hacker hobbyists looking for glory and free digital content is now the realm of criminally minded professionals. For years, IT administrators viewed most malware as more of a nuisance than something that could inflict lasting, six- and seven-figure damage. In years past, malware might leave "greetz" messages to other hackers in their code, set up file-trading sites or open IM chat channels, not anymore. Today's top threats are professionally written programs coded to steal identities and passwords, break into restricted Web sites, conduct corporate espionage, and install Spyware (Grimes, 2005, p. 23).

Current programs infecting computers no longer just seek to boost a programmer's ego or leave a message or even destroy files. The latest round of infections seeks to remain unknown so that criminal activities can be undertaken. (Grimes, 2005) further notes:

> The malicious programs now making the rounds leave corporate administrators wishing for the days when viruses and Trojans were relatively simple and benevolent, and when intrusive code was removed after the crisis was over. With much of today's malware, the initial infection vector is only the setup and data destruction is the least of the administrator's worries. After a computer has been exploited successfully, many worms and bots will connect to outside servers and download new programs or instructions. Using

> this "mothership approach" the malware becomes self-updating. Its eventual instructions are never known- many times, even to the code's writer- until it has run its course (Grimes, 2005, p. 23-24).

To defend against these security threats several steps need to be taken, which include multi-layering defenses, make further use of heuristics, and educating the end user.

With this background in mind the next section focuses on security problems on a college campus.

2.2 Security Problems on a College Campus

An institution of higher learning is a location you would expect to be up to date on security issues and have a security policy in place. Contrary to that expectation college and university campuses are among the least secure computer environments. Multi-media learning are a technique that is quickly infiltrating the classroom. Techniques from requiring word processed documents to be submitted to power point presentations along with distance learning all introduce the student to a computer, a network, and the Internet. This creates need for security. With suggestions on minimizing security risk in a classroom (Ozkan & Gunay, 2004) makes these observations:

> Today it is common practice for most universities to use networked computers that enable users to communicate freely with each other. However, only a few students, faculty members and administrators are aware of the risks and vulnerabilities that exist in their network operating systems. Dr. E. Eugene Schultz, a principal engineer at the Berkeley National Laboratory and Editor-in-chief of *Computer & Security,* reports that universities are "among the least secure places in the universe as far as computing goes" (Foster 2004). This is because most colleges do not perform risk assessments of their network systems,

> and many administrators do not periodically review their policies as required by federal regulations. In addition, students often are not fully aware of the need to use anti-virus programs or how to properly use copyrighted materials, and faculty members frequently assume that computers in their offices are secure (Ozkan & Gunay, 2004, p. 32).

Students, instructors, and administrators may not even fully understand that security risks, especially virus proliferation employ many methods of delivering the virus to a computer. Some of the more common methods other than email include, CDs, floppy disks, USB storage devices, scanned copies, WebCT, Blackboard, and networked drives (Ozkan, 2004 p. 34)

The SOT at Eastern Illinois University employs many of these methods of instruction. WebCT is frequently used by the SOT and is expanding in use as the off campus program grows. The use of other devices such as CD's and USB storage devices places the SOT in the area of risk for virus or worm infections.

One effort taken by State University of West Georgia is to provide free assistance to students that may not otherwise be able to afford to pay for a virus to be removed from their computer. The service called Student Information Technology Services (SITS) repairs and otherwise assists students with technology problems (Ozkan, 2004 p. 36). The value of this service is that it removes a potential source of further infection on the universities networks or in the dorms.

SOT students at Eastern Illinois University have a similar location where they can seek assistance. The Information Technology Services Help Desk at http://www.eiu.edu/~itshelp/ provides helpful information. The following statement of purpose is provided:

> Whether you are a student needing a password reset for your EIU e-mail account, a faculty member searching for WebCT support, a staff employee whose PC is malfunctioning or

> any member of the university community in need of any kind of help with your computer, you can get assistance by stopping by the easily accessible Gregg Triad location or simply calling 581-HELP (4357).

In a manner similar to the State University of West Georgia the value of this service is that it removes a potential source of further infection on the universities networks or in the dorms.

Universities present unique challenges for security implementation. The varied nature of tasks that need to be accomplished in a university setting presents a complex set of problems for the security professional. On a college campus there are found libraries, museums, laboratories, experimental work, retail establishments, and other cash handling operations. Add to these operations the confidential data that exists on a college campus. Data such as social security numbers, health information, and student loan information. With such varied levels of security needed it is understandable how a university may encounter security problems. (Phelps, 2004) suggests:

> To establish an effective security program, one first must be aware of the environment in which he or she is operating. Security may be the only program that each of the departments is working on together. In many cases, it may be best to form a security advisory board, with members from each school or department, which can help unify the campus program (Phelps, 2004, p. 50).

Eastern Illinois University faces a number of these same challenges. The library provides access to the Internet as well as providing a wealth of literature. Online registration, online tuition payment, and online records all need to operate within a secure environment.

A major step toward a secure environment is cooperation within the organization or in the case of a university, an institution. Understanding that research may require more freedom than

perhaps securing a student financial or health information is a beginning toward a secure campus. Taking the needed steps to separate these information sources and providing the level of security needed is essential.

The cost of an infection of a virus can be staggering. (Foster, 2004) present's data about the cost of a virus as follows:

> The informal survey of 19 research universities shows that each spent an average of $299,579 during a five-week period last summer to undo the havoc wrought by the so-called Blaster worm. (It got its name from MSBlast.exe, the file that the worm created on infected computers.) Nationwide data about the cost of worms and viruses to colleges contacted by The Chronicle say the costs are high and growing.

The costs at affected universities may go even higher. (Foster, 2004) states:

> Of the universities surveyed, the University of Colorado at Boulder spent the least: $9,000 to repair 265 infected computers. Stanford University spent the most: $806,000 to repair 6000 computers. Sandi Senti, executive director for technology strategy and support at Stanford, said the university spent 18,420 hours rebuilding machines. Because the institution has a medical school with sensitive health data, Ms. Senti decided that patching infected computers, a cheaper option, would not suffice (Foster, 2004, p. 30).

This situation just required rebuilding machines; other occurrences have exposed confidential data which also require notification of any persons that may have been affected. The costs of this notification process along with associated liabilities can send potential costs sky rocketing. For a business the loss of confidence by consumers could affect business for a substantial time, especially if e-commerce is part of their business.

To prevent the spread of such virus and worm infections many universities have taken a proactive posture. (Foster, 2004) highlights an array of approaches that some universities have enacted as follows:

> Colleges are also stepping up efforts to get campus computer users to do a better job of protecting their machines. Some institutions, such as Connecticut College, require all students to install antivirus software on individually owned computers, but officials expect students to purchase and install the software on their own. And Mr. Hisle, the college's information-resource vice president, acknowledges that the rule is not enforced. "We are working on software that will allow us to scan the student machines and determine whether or not they've got up-to-date protections," he says. "But that's not in place yet. We just don't have time to do it." The scanning process involves identifying the operating system on each student's computer, then checking to see if the latest patches for that system have been installed. If the patches are not there, university technicians can make sure they are added before the computers are connected to the university network. Such scanning is already in place at some colleges, including the University of Colorado at Boulder. ... Mr. Maloney says that thanks to the scanning process, he prevented 40 percent of the roughly 6,000 computers that Boulder students brought to the campus from becoming infected or spreading infections. Many colleges have gone beyond just requiring student's machines to have antivirus software; they provide the software free (Foster, 2004, p. 30-31).

Eastern Illinois University has adopted a position similar to that of the University of Colorado at Boulder where scanning of student computers for security software is performed before allowing the computer to connect to the network. This is done as a protective measure for the school's network.

The risk is real and the costs associated with a security breach run high so security management is quickly becoming a priority in the business world as well as the academic world.

2.3 Security Management

Managing security takes several forms; there is software and hardware available to accomplish the task. Eastern Illinois University's policies and procedures include several features that are on the breaking edge of technology. Software includes antivirus programs, Adware removal programs, Spyware removal software, and built in security measures within most operating systems. Hardware options include firewalls and email filters such as a Barracuda's email filter.

2.3.1 Firewalls

Students within the SOT at Eastern Illinois University have many options of technology to include within their security arsenal. One of the devices is the firewall; the firewall can be an appliance that is moderately simple or very complex. A firewalls initial job was to simply grant access or not grant access by allowing traffic to flow through to the protected network or denying access. The data travels in small pieces of information called packets. When information is transferred data are broken down into these packets and a header is placed with the packet so all the data can be reassembled when the destination is reached. The problem, however, has developed whereby hackers can access these packets and place data within these packets that could later be harmful. The basic firewall has no method of assessing whether the packets are safe or not. Firewalls have been expanded to include what is known as deep packet inspection. Such firewalls are able to look at packet information and determine patterns, thereby preventing attacks from hackers.

Simply the word firewall creates apprehension in many persons. The perception of complexity of the firewall can create an aversion too many end users. User friendliness is essential if this technology is going to benefit the end user. An examination of several firewalls emphasizes the user friendliness or lack thereof. The technology as being developed seems to point toward more user friendliness. End user behavior is a vital consideration when examining the issues associated with security and how to manage the security measures applied in each situation.

InfoWorld (Rist & Rash, 2003, pp. 38-40) published an article where an attack was simulated on four different firewalls and each was then evaluated for speed, effectiveness of handling the attack, a cost value comparison, and ease of configuration. The four models selected were EnterasysXSR-3250 Security Router, Ingate firewall 1400, Nokia IP380, and the Toshiba Magnia SG20. The testing methods used were Communications' Ixia 1600 traffic generation chassis and Web load testing software. The testing software generated real world traffic flow and simulated attacks (Rist & Rash, 2003, pp. 38-40). A troublesome aspect to firewall security is configuring the firewall to ensure a secure network. In the early models of the firewall configuring the appliance was accomplished through a command line. In most cases the ability to perform the task required expertise in the operating system used by the manufacturer.

In view of the cost and continuous management required for a secure network Fonseca in (Rist & Rash, 2003, p. 43) presents another alternative for small to medium size businesses. He shows that some companies have decided to employ the use of a MSSP (managed security service provider). The MSSP will provide the following for businesses as Fonseca notes in (Rist & Rash, 2003, p. 43):

> ... prompting some companies to off-load security responsibilities onto the shoulders of MSSPs (managed security service providers), vendors that provides configuration and management expertise, and even around the clock monitoring, along with their security solutions.
>
> Of course MSSPs, which include the likes of AT&T, Guardent, IBM, Internet Security Systems (ISS), Symantec, and TruSecure, want to manage more than your firewall. Their services run the gamut, from vulnerability assessment and remediation, to managing anti-virus gateways and VPNs, to complete security-policy management and intrusion detection. Vendors at the high end, such as Guardent, even offer incident-response and forensics services
>
> But it is often the complexities of firewall configuration, and the challenges involved in securing the network edge, that lead most managers to turn to MSSPs (Rist & Rash, 2003, p. 43)

Clearly firewalls present difficulties for even experienced IT personnel. Although efforts to enhance configuration issues are underway there is still a need for improvement for these devices to be usable for the small business or home user to take advantage of this measure of security. The network world is in a constant state of change and firewalls must change with it. For example VOIP (Voice over IP) is a new technology that firewalls has not been designed to handle. IDS (Intrusion detection systems) are necessary for a secure network. These are issues that the next generation of firewalls will be required to monitor as well. In a survey of seven leading firewall suppliers when asked to define what was meant by next-generation firewall and its market this response was received.

Ingate, Nortel, and SecureLogix say that deep packet inspection will become common. Ingate and Avaya believe that encrypted transmission of signaling and content will be supported.

But when encryption is used, it will limit or eliminate the participation of the firewall in the signaling process (H.323, SIP, and MGCP) - the firewall will not be able to perform deep packet inspection of encrypted packets. The choice will be encryption or deep packet inspection, not both at the same time.

All the respondents agree that whatever processing occurs, performance cannot be degraded. The next-generation firewall must process traffic at wire speed (Audin, 2004, pp. 57-58).

Not all firewalls are hardware appliances. Firewalls come as software (e.g., SystemWorks from Symantec Corporation). SystemWorks is inexpensive at $75-$100. This product offers antivirus protection and a firewall. Other utilities come with the package that helps keep your computer running smoothly. (Miastkowski, 2001) in PC World states: "Symantec has made the firewall setup process much easier. A wizard provides extensive explanations as it guides you through the crucial steps. Much of the configuration of Internet-accessing applications is now automatic" (Miastkowski, 2001, p. 68).

Other software firewalls are available and Microsoft Windows XP service pack 2 has a firewall embedded in its operating system. There are built-in firewalls available with broadband routers as (Wilson 2005) notes:

Home users can get built-in firewalls with their $69 broadband routers and wireless access points, and sometimes they even turn these on, but the products typically lack many features of enterprise-class firewalls. Advanced features like virus scanning, spam filtering and intrusion protection are gradually being commoditized and will likely trickle down in the next year or two to home users. Many small and medium organizations are in a situation similar to home users, in that the products they can afford or are willing to spend money on aren't necessarily capable of

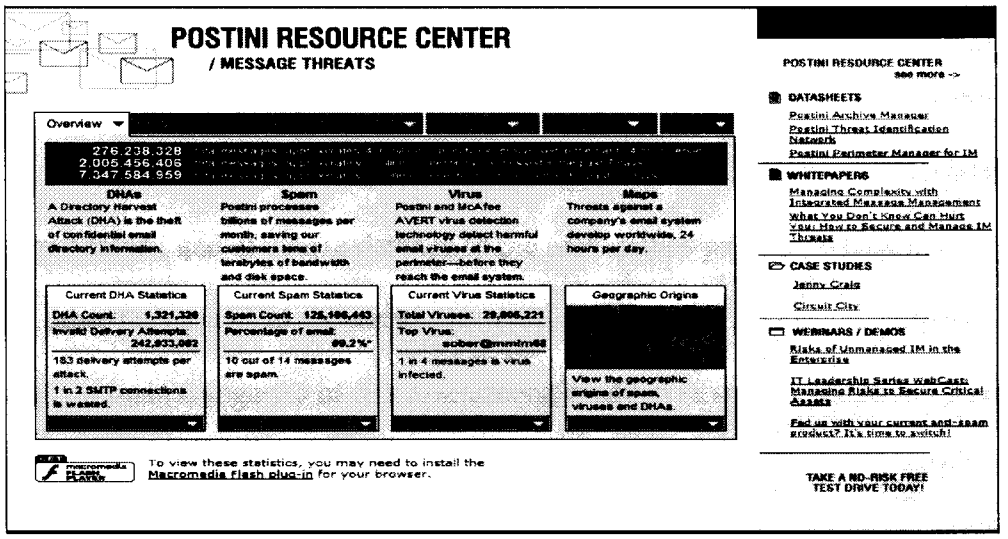
protecting from today's sophisticated attacks.... For these customers the coming generations of routers may be the easiest way to get good protection, as they will have built-in enterprise-class security technology (Wilson, 2005, p. 29).

2.3.2 Email Filters

Transferring security threats through email has been a common practice with computer viruses and worms. The usual, best practice is that if you do not know the sender or are not expecting an email from a certain source then delete the message and attachment. However, this is not always practical, especially in a business or academic setting. The use of anti-virus software and other appliances has reduced the transfer of malware by this means; however unwanted emails have increased exponentially. The common term for these unwanted emails is spam.

There are several options for filtering email. One option is to use an email filtering service. There are many of these services available. Some companies use these services to reduce management and administration costs. These services also combine anti-virus protection as part of the service. While this should not be the only anti-virus protection used, it does provide an additional layer of protection. One such provider of this service is Postini. Note these statistics from their Website.

Figure 2-1 Postini Resource Center



(Postini Integrated Message Management, 2005) http://www.postini.com/stats/

Other providers provide similar services.

A second option for spam filtering is software which is installed on the PC of the end user. Many home users find this provides some relief from spam. Software applications such as Symantec offer packages that contain this service. Norton AntiSpam 2005 is one such product (Symantec, 2005).

The third option is a hardware appliance such as the Barracuda. The Barracuda is an email filter that works in several ways. One way is by using blacklists. These lists provide known senders of spam. Another way is based upon spam scoring. A final way is that the end user is able to mark a sender as spam and thus create a personal blacklist, preventing further emails being allowed to pass through the appliance. The user is also able to define a whitelist which allows email that may have been scored as spam to pass through.

Eastern Illinois University is currently using this particular type of spam management. In fact Eastern Illinois University is using the Barracuda appliance.

2.4 Need for Risk Assessment

With liabilities at such a high level organizations regardless of size should have some form of risk assessment of their security measures performed. The liabilities involved for a university include loss or theft of confidential data, destruction or theft of files including research being conducted by professors, and of course damage to the universities property which include computers and other technological property.

There are two main categories of risk assessment, qualitative and quantitative. (Karabacak & Sogukpinar, 2005) discuss these methods:

> Basically there are two types of risk analysis methods. Quantitative risk analysis methods use mathematical and statistical tools to represent risk. In qualitative risk analysis methods, risk is analyzed with the help of adjectives instead of using mathematics. Risk analysis methods that use intensive quantitative measures are not suitable for today's information security risk analysis... Because qualitative methods do not use tools like mathematics and statistics to model the risk, the result of method is vastly depended on the ideas of people who conduct the risk analysis (Karabacak & Sogukpinar, 2005, p. 148).

Karabacak & Sogukpinar focus their risk procedure on the Information Security Risk Analysis Method (ISRAM). ISRAM is based on the following formula:

Risk = (Probability of occurrence of security breach) X (Consequence of occurrence of security breach)

(Karabacak & Sogukpinar, 2005) summarizes ISRAM as follows:

> In this study, a novel method, ISRAM, is proposed for information security risk analysis. The proposed method is based on a quantitative approach that uses survey results to analyze information security risks.

Quantitative tools included in ISRAM are simple numbers related with the survey, risk tables, addition, multiplication, and division operations. The main advantage of ISRAM over other risk analysis methods is its ease of use. There are no complicated mathematical and statistical instruments in ISRAM (Karabacak & Sogukpinar, 2005, p. 158).

Previously, it was mentioned that qualitative methods might give subjective results. ISRAM is a quantitative tool with well-defined steps and mathematical measures. With a careful operation, ISRAM gives objective risk results.

Universities would be able to perform such a risk analysis. As the threat to these institutions creates the risk of higher costs liabilities, more universities will perform some sort of risk analysis.

While a risk analysis is normally performed by businesses and organizations such as Eastern Illinois University, students may not see a need for a personal risk analysis. Students within the SOT might well consider a qualitative analysis of their personal risk. When considering the probability of data loss and comparing that to the value of what could be lost the student may find there is more to lose than initially thought.

2.5 Advancing Security Concerns

Technology is advancing at a very fast pace. Change is constant and new technologies appear on nearly a daily basis. In recent years wireless technology has exploded and is becoming a widely used technology. Voice over IP (VOIP) is a new technology as well, and presents more opportunity for both the technology user and those that seek to perform criminal activities. Other new technologies include data transmission over electrical lines. Adding these to the current technology that is constantly in a state of change presents serious security issues to be resolved. Those who work with security have a daunting task because with heavier reliance on technology

and more financial liabilities the criminals who present security problems receive a larger payoff when an attack is successful.

2.6 Security at Eastern Illinois University

Eastern Illinois University has an established Computer use policy which can be viewed in detail at http://www.eiu.edu/~infotech/Policy/policy.php . The information here states in part:

> Information Technology Services provides computing facilities and services for the legitimate instructional, research, and administrative computing needs of the university. Proper use of those facilities and services supports the legitimate computing activities of Eastern Illinois University students, faculty and staff. Proper use respects intellectual property rights.
>
> Legitimate instructional computing is work done by an officially registered student, faculty, or staff member in direct or indirect support of a recognized course of study. Legitimate research computing is work approved by an authorized official of a university department. Legitimate administrative computing is work performed to carry out official university business (Eastern Illinois University, 1998).

In section 2.2 (Foster, 2004) is cited as saying:

> Colleges are also stepping up efforts to get campus computer users to do a better job of protecting their machines. Some institutions, such as Connecticut College, require all students to install antivirus software on individually owned computers, but officials expect students to purchase and install the software on their own. And Mr. Hisle, the college's information-resource vice president, acknowledges that the rule is not enforced. "We are working on software that will allow us to scan the student machines and determine whether or not they've got up-to-date protections," he says. "But that's not in place yet. We just

> don't have time to do it." The scanning process involves identifying the operating system on each student's computer, then checking to see if the latest patches for that system have been installed. If the patches are not there, university technicians can make sure they are added before the computers are connected to the university network. Such scanning is already in place at some colleges, including the University of Colorado at Boulder (Foster, 2004, p. 30).

Eastern Illinois University has implemented in the fall semester 2005 a security measure called Clean Access Agent which performs tasks similar to what is described as taking place at University of Colorado at Boulder. This software ensures that computers logging onto the University's network has antivirus software and that the computer has the latest antivirus definitions. The software also checks the computer attempting to connect to the network for Microsoft critical updates and that automatic updates is enabled. Users are required to log in to the network at specified maximum intervals to allow these checks to take place. Further, Eastern Illinois University has implemented an email spam filter to further eliminate spam and potential virus infections. Eastern Illinois University, by implementing this program is proactive in helping students protect their computer. The website http://mypc.eiu.edu/ is a site where Eastern Illinois University provides downloads needed to install antivirus software and other protective measures. If critical updates are needed a student is directed to the proper location to download these updates.

The provisions of Clean Access Agent along with various websites and an IT helpdesk places Eastern Illinois University as a proactive participant in helping students maintain a secure computer environment.

Chapter 3

Research Method

The Internet continues to expand each day and provides access to knowledge and information to persons that seek to broaden their understanding yet security risks associated with the Internet are increasing. Information is a key facet to students and for individuals wanting to either expand their knowledge about a subject or perform research over the Internet. Many day to day transactions, such as banking and purchasing merchandise takes place over the Internet. The Internet opens a world of information for students and researchers that only a decade or two ago would not have existed.

The value of the Internet for individuals and the student or researcher is beyond question. Along with the advantages of the Internet come associated risks. These risks include viruses, worms, denial of service attacks, and data theft. An attack from any of these methods to infiltrate or damage a network or computer can be extremely costly.

The current technology in solving the problems associated with these attacks is the use of firewalls. Firewalls attempt to block access to networks or computers that reside behind the firewall. Firewalls currently exist in two main forms. There are firewall devices or appliances which are actual pieces of hardware and there are firewall software packages. Also available are anti-virus software program which will block a large number of known viruses and worms, but do little to prevent intrusion attempts or other forms of hacking.

Universities have taken note of the problems and security issues associated with computers and the Internet. Some universities have provided technical expertise; others provide software to assist the student in maintaining their computers in a state where a student's computer is exposed to minimal risk. Other universities have set regulations and enforce a minimum state of security

protection for a student's computer. Some universities even scan student computers to enforce compliance with security requirements.

Students may not be aware of the problems associated with an inadequately secured computer. Further students may not be fully aware of tools available and steps to take as a user to protect their computers. Eastern Illinois University takes a proactive position in regard to security. Some of the options that SOT students may avail themselves of is Symantec anti-virus software, Ad-aware, and Spybot as direct security software for anti-virus protection and Spyware detection. Eastern Illinois University also has employed the use of an email filter device called Barracuda which provides additional spam detection. With so many services available the purpose of this study is to identify the perceptions of students attending the School of Technology at Eastern Illinois University regarding computer security. Based on the student perceptions this study may be able to assist Eastern Illinois University officials in determining if further measures are needed to provide a secure environment for students.

3.1 Participants

The School of Technology offers degrees in four main areas. The school offers a B.S. (Bachelor of Science) in Industrial Technology, a B.S in Career and Technical Education, a B.S. in Career and Organizational Studies, and Graduate Studies in Technology. The participants represent respondents from each of these degree programs. Ten classes were surveyed. They were INT 2523: Routing and Switching Fundamentals, INT 4274: Automation and Control, INT 2324: Electronic Control Systems, CTE 2000: Inquiry into Teaching Career and Technical Education, CTE 3100: Instructional Technology in Career and Technical Education, COS 4850: Coaching and Mentoring For Supervisors, TEC 5103: Science and Technology of Leadership, TEC 5133: Total Quality Systems, TEC 5723: Issues and Trends in Technology and TEC 5243:

Design For Quality. These classes were chosen to provide a representation of the School of Technology at Eastern Illinois University and they were made available by the professors. The School of Technology has an enrollment of 586 students during the fall 2005 semester. From these classes there were 133 respondents which represent 22.7% of students enrolled in the School of Technology during the fall 2005 semester.

3.2 Procedure

The procedure for this research presented a survey that contained 25 statements about computer security which was completed by the students during one of their class sessions. Once the surveys were completed the data was compiled and analyzed.

3.3 Instrument

The survey was based on a likert scale with statements ranging from strongly disagree which was equal to 1 to strongly agree which was equal to 5. The statements focused on availability and access to security measures, information provided during student orientation, and technical assistance made available to the students. As a result of the survey four statement grouping appeared to emerge. These grouping were End User Related: Actions, End User Related: Understanding, Hardware/Software Related, and Eastern Illinois Related. The groupings of End User Related: Actions and End User Related: Understanding appeared to relate closely with security behaviors identified in the Two Factor Taxonomy table, table 2-1. The Hardware/ Software grouping of questions took form as firewalls and virus protection measures were examined. Rist & Rash examined this area closely with their examination of several firewalls. The fourth grouping of questions, Eastern Illinois Related stood out as a result of a consideration of measures Eastern Illinois University applied. For further discussion of the measures see Appendix B

3.4 Data Analysis

The data collected from the survey was used to determine the perception of the respondents in regard to the effectiveness of university provisions, technical support and training available to the student. The collection of data from these classes with 133 respondents included the four areas of study within the SOT, providing the data for this study.

By examining the mean score of the respondents with the possible range from 1 to 5 and letting a mean of 1.000 to 2.333 represent the perception that the respondent strongly disagrees and a score of 2.334 to 3.670 represent no strong opinion either agreeing or disagreeing and letting 3.671 to 5.000 represent a strong agreement we should be able to determine the perceptions regarding the effective use of software or other security provisions made by the university.

Chapter 4

Results and Discussion

There were 133 respondents to the survey containing 25 statements reflecting, end user actions, end user understanding, hardware and software applications, and regarding Eastern Illinois University.

4.1 Results

Table 4-1 Statement Means and Standard deviation

Statement #	Mean	Std. Deviation	Statement #	Mean	Std. Deviation
1	4.774	0.667	14	3.624	1.318
2	4.135	1.002	15	4.180	1.116
3	4.075	1.073	16	3.233	1.584
4	4.669	0.849	17	3.098	1.537
5	4.278	1.197	18	3.105	1.457
6	3.985	1.387	19	2.553	1.372
7	2.436	1.373	20	2.504	1.616
8	1.895	1.203	21	1.682	1.263
9	3.947	1.400	22	3.273	1.402
10	4.226	1.001	23	3.910	1.102
11	3.500	1.323	24	3.386	1.363
12	3.439	1.389	25	3.545	1.029
13	2.227	1.329			

This study is descriptive in nature, identifying perceptions of the respondents. For this reason and the fact that several of the survey statements had the natural response of 1 or 5 the

standard deviation of some of these statements appeared to have less meaning when applied to the statement. Comments about the standard deviation have been included in the discussion of the statements where it appeared to have meaning.

Survey Statement 1:

I am aware that computer viruses can infect my computer in the following ways: through opening an infected email, through an infected floppy disk, through visiting an infected website.

The mean for this statement was 4.774 indicating an agreement to strong agreement from the respondents. By indicating an agreement to strong agreement to this statement students in the SOT at Eastern Illinois University appear to understand several methods of possible computer virus infection.

For the extent of this research the results appear to differ from what Ozkan (2004) states:

> Students, instructors, and administrators may not even fully understand that security risks, especially virus proliferation employ many methods of delivering the virus to a computer. Some of the more common methods other than email include, CDs, floppy disks, USB storage devices, scanned copies, WebCT, Blackboard, and networked drives (Ozkan, 2004 p. 34)

Survey Statement 2:

I always protect my user passwords for my computer and any computer accounts I may have access to.

The mean for this statement was 4.135 indicating an agreement to strong agreement from the respondents. By agree to strongly agreeing to this statement the respondents fit well into the category of the two factor taxonomy of security behaviors table where expertise is low and

intentions are beneficial. The table formulated in a study by Stanton (2005) attempts to identify end user security behaviors. (Stanton et al., 2005, p. 126)

Survey Statement 3:

I never share my password with my friends or associates.

The mean for this statement was 4.075 indicating an agreement to strong agreement from the respondents.

This end user activity and result relates in the same manner to the two factor taxonomy table as statement 2. Perhaps even without realizing that it was happening the respondent performed a risk analysis of a qualitative nature (Karabacak & Sogukpinar, 2005).

Survey Statement 4:

I have an anti-virus software installed on my computer.

The mean for this statement was 4.669 indicating an agreement to strong agreement from the respondents. This software related statement indicates that most of the respondents do have anti-virus installed on their computers. For students that connect to the university's network this is enforced by software. For this reason the results from this statement would seem to disagree with Furnell which stated:

> Based upon a sample of 329 homes (59% using broadband access and 41% using dial-up connections) the study determined a number of worrying findings. For example, more than half of the respondents were not clear on the difference between anti-virus and firewall protection. Moreover, many of them were not using the technologies effectively – a scan of the respondents' systems revealed that 67% either had no anti-virus software on their system at all or had not updated it within the previous week and 72% lacked a properly configured firewall (Furnell, 2005, p. 275).

Survey Statement 5:

I either update my anti-virus software weekly or have the software configured to do so.

The mean for this statement was 4.278 indicating an agreement to strong agreement from the respondents. This software related statement indicates that most of the respondents do have the anti-virus on their computers set to update definitions weekly or do so manually. For students that connect to the universities network this is enforced by the Clean access Agent.

Survey Statement 6:

I use a firewall on my personal computer.

The mean for this statement was 3.985 indicating an agreement to strong agreement from the respondents. Firewalls exist in two forms, either as software or as a hardware appliance. This statement did not establish a difference between the two. However the respondents did indicate an awareness of the existence of a firewall associated with their computer. With Windows XP service pack 2 there is a firewall associated with the operating system. More devices are being equipped with firewall and antivirus software as part of the device package. New areas have been exposed for potential threats including E-Business and those that employ the use of wireless services (Hulme, 2004, p. 67).

Survey Statement 7:

If I have an anti-virus software I am guaranteed to not be infected by a virus.

The mean for this statement was 2.436 indicating neither a strong agreement nor strong disagreement from the respondents. The response neither a strong agreement nor strong disagreement indicates a possible lack of awareness that new computer viruses can cause problems before the anti-virus software is able to protect the computer.

Survey Statement 8:

Computer viruses and worms are the only security risks I need to be concerned with.

The mean for this statement was 1.895 indicating a disagreement to strong disagreement from the respondents. The disagreement to strong disagreement to this statement indicates an awareness of threats beyond viruses. Malware has gone beyond being a nuisance, presenting far greater threats. Currently the concerns threats of an infection has mutated from a fear of losing data and damage to hardware or an operating system to an unidentified infection that allows a computer to be used for multiple purposes without the owners knowledge. Grimes indicated one of the dangers:

> The malicious programs now making the rounds leave corporate administrators wishing for the days when viruses and Trojans were relatively simple and benevolent, and when intrusive code was removed after the crisis was over. With much of today's malware, the initial infection vector is only the setup and data destruction is the least of the administrator's worries. After a computer has been exploited successfully, many worms and bots will connect to outside servers and download new programs or instructions. Using this "mothership approach" the malware becomes self-updating. Its eventual instructions are never known- many times, even to the code's writer- until it has run its course (Grimes, 2005, p. 23-24).

Survey Statement 9:

It is possible for my computer to be infected and I would not realize it.

The mean for this statement was 3.985 indicating an agreement to strong agreement from the respondents. The agreement to strong agreement to this statement indicates awareness that destruction may not be the only purpose of an infection.

Survey Statement 10:

I understand that new viruses and worms may reside dormant until a later time.

The mean for this statement was 4.226 indicating an agreement to strong agreement from the respondents. This end user related statement indicates by the agreement to strong agreement from the respondents that an infection could be triggered at a time later than the initial infection.

Survey Statement 11:

I know the policies established by Eastern Illinois University regarding computer security and abide by them.

The mean for this statement was 4.226 indicating an agreement to strong agreement from the respondents. This statement is related to end user actions. The response to this statement indicates that respondent's feel they know the policies established by Eastern Illinois University and that they follow those policies. This differs from what Furnell found in his respondents. "For example, more than half of the respondents were not clear on the difference between anti-virus and firewall protection. Moreover, many of them were not using the technologies effectively..." (Furnell, 2005, p. 275). Possible reasons for this difference include the population being sampled and methods that Eastern Illinois University employs to educate their students.

Survey Statement 12:

I use security measures made available by Eastern Illinois University.

The mean for this statement was 3.439 indicating neither a strong agreement nor strong disagreement from the respondents. This end user action indicates some room for improvement. In the area of security Eastern Illinois University would like to see a strong agreement in response to this statement. Some measures are enforced by Eastern Illinois University others are optional relying on the end user to make proper use of what is provided. There may be room for

further education of what is available and possible further training about security may be an option to improve the use of what Eastern Illinois University provides.

Survey Statement 13:

During orientation I was provided information about computer security and what Eastern Illinois University requires.

The mean for this statement was 2.227 indicating a disagreement to strong disagreement from the respondents. The perception of the respondents indicates that there may be some room for educating incoming students regarding computer security policies.

Survey Statement 14:

I would like more information to be provided by Eastern Illinois University about what I could do as a student to maintain a secure computer.

The mean for this statement was 3.624 indicating neither a strong agreement nor strong disagreement from the respondents. This statement regarding perceptions about Eastern Illinois University's actions while falling within the neither strongly agree nor strongly disagree range does so at the high end. The standard deviation of 1.318 indicates mixed perceptions about the amount of information provided by Eastern Illinois University. This mean and standard deviation shows a relatively flat curve which is another indication of mixed perceptions.

Survey Statement 15:

If I were provided software by the university I would install and keep the software updated.

The mean for this statement was 4.180 indicating an agreement to strong agreement from the respondents. The agreement to strong agreement to this statement indicates willingness on the part of the end user to be proactive and help secure their computer and thus help maintain a secure network for the University. Eastern Illinois University does make provision in this area

and awareness and education regarding the use of the software may be a key factor in maintaining a secure computer environment.

Survey Statement 16:

I have lost data of some form due to a computer virus or a security breach.

The mean for this statement was 3.233 indicating neither a strong agreement nor strong disagreement from the respondents. This statement had the second largest standard deviation at 1.584 indicating respondents had lost data and others had not. While the amount or type of data lost is not indicated it is indicated that many have lost data of some sort. That data could have been very important or may have been of minimal importance. The important determination from this statement is that data loss does occur and a number of the respondents in this study had suffered such a loss.

Survey Statement 17:

I have never tried to access a secure area on a network.

The mean for this statement was 3.098 indicating neither a strong agreement nor strong disagreement from the respondents. The response to this statement while in the range of no strong agreement indicates that a substantial number of the respondents had tried to access a secure area. This end user activity fits in well with the Two-factor taxonomy of security behaviors table. The intentions can not be determined to be beneficial or detrimental with the information provided, however the action of the end user does show intentionality.

Survey Statement 18:

If I had the technical knowledge I would consider accessing a secure area.

The mean for this statement was 3.105 indicating neither a strong agreement nor strong disagreement from the respondents. This statement is closely related to statement 17 and similar perceptions can be drawn.

Survey Statement 19:

I have unknowingly accessed a secure area on a network.

The mean for this statement was 2.227 indicating a disagreement to strong disagreement from the respondents.

Survey Statement 20:

I have received the password of a classmate, co-worker, or associate.

The mean for this statement was 2.504 indicating neither a strong agreement nor strong disagreement from the respondents.

Survey Statement 21:

If I received a phone call from someone claiming to be from Eastern Illinois Universities IT department I would give them my password if requested.

The mean for this statement was 1.682 indicating a disagreement to strong disagreement from the respondents. This end user action indicates a good understanding of the dangers of releasing their password. Standard security practice is to never give your password to another person. In most situations the person in authority of a network would not ask for a password. If asked the person should instantly perform a risk analysis of a qualitative nature. Asking what consequences could follow (Karabacak & Sogukpinar, 2005).

Survey Statement 22:

My wireless router is properly configured to prevent access by unauthorized persons. If you do not have a wireless router please leave blank.

The mean for this statement was 3.273 indicating neither a strong agreement nor strong disagreement from the respondents. Of the 133 respondents 77 responded to this statement and the responses fell within the neither strongly agree nor disagree range. So some respondents have a secured wireless network and others do not. This hardware related statement indicated a need for further education both in regard to the threats of an unsecured network and in regard to the method to enable security measures on a wireless network.

Survey Statement 23:

I have a good understanding of computer security and measures needed to protect my computer and data.

The mean for this statement was 3.910 indicating an agreement to strong agreement from the respondents.

Survey Statement 24:

I would like to receive additional training in regard to computer security and resources available from Eastern Illinois University.

The mean for this statement was 3.386 indicating neither a strong agreement nor strong disagreement from the respondents. The standard deviation for this statement was 1.363. With this in mind it is indicated that there may be quite a number of respondents that would like to receive additional training.

Survey Statement 25:

Rate your level of computer technical expertise where 5 is high level of expertise and 1 is a low level of technical expertise

The mean for this statement was 3.545 indicating neither a strong agreement nor strong disagreement from the respondents. This response is just near the top of the neither strongly

agree nor strongly disagree range indicating that a small majority of respondents consider their computer expertise above the average.

4.2 Statement Grouping

The statements within the survey can be classified into four basic areas. There are two end user areas, one is end user related actions, and the other is end user related understanding. The other two areas are hardware/software related statements and the final area is Eastern Illinois University related statements. These groups of statements are as follows:

Table 4-2 Statement Grouping

Statement Group	Statement
End User Related: Actions	2,3,11,12,15,17,18,19,20,21
End User Related: Understanding	1,7,8,9,10,23,25
Hardware/Software Related	4,5,6,16,22
Eastern Illinois University Related	13,14,24

By examining the responses to these statements within the context of the statement groups the perceptions of the respondents become clearer.

End User Related: End user actions are a key to computer security. The study by (Stanton et al., 2005) resulted in the Two Factor Taxonomy of Security Behaviors which examines in depth behaviors of end users. The study concentrated on intentionality and expertise. Stanton expands on this:

> By collapsing across the many similarities among these expert-generated categories, we developed a six element taxonomy of security behavior that varied along two dimensions: intentionality and technical expertise. The intentionality dimension appeared to capture whether the behavior described was intentionally malicious, intentionally

beneficial, or perhaps somewhere in between (i.e., absent explicit intention to help or harm). The technical expertise dimension focused on the degree of computer or information technology knowledge and skill that the actor needed to have in order to perform the behavior described on the card (Stanton, Stam, Mastrangelo &, Jolton, 2005, p. 126).

Statements in this grouping had the largest number of statements on the survey. Generally the responses indicated that good security practices were in place. Specifically with regard to password protection as exhibited in statements 2,3,20, and 21. Statements 17 and 18 indicated there could be some security issues from the respondents in accessing areas that were deemed to be secure. Statements 12 and 15 indicate a concern with maintaining security on their personal computer.

End User Related: Understanding is important to maintaining security. Interestingly Stanton's research indicates that within the six element taxonomy, security directly relates to intentions and technical abilities. The range described in the Two Factor Table, Table 2-1 range from destructive with high expertise to low expertise with obvious intent to preserve security. The responses of the survey indicated an excellent understanding in general as indicated by responses to statements 1,7,8,9, and 10. The responses to statements 23 and 25 even though the agree to strongly agree range, indicates a mixed perception of the respondents own understanding of computer security.

Hardware/Software related statements indicate some work is left to be accomplished as indicated by the respondent's perceptions. The use of anti-virus software and for most a firewall signifies excellent use of software/hardware and responses to statements 4, 5, and 6 indicate. The area of concern is highlighted by the responses to statements 16 and 22. These responses indicate

that some have lost data and that some may be using a wireless device that may not have security features enabled.

Eastern Illinois University Related Statements indicate that many would like more information about computer security. This grouping of statements helps identify areas where Eastern Illinois University may have an influence regarding the perceptions of students in the SOT. This is highlighted by responses to statement 13. It could be that more information may not be needed but rather information on how and where to access such information. Statements 14 and 24 seem to indicate some would and some would not like more information or training in regard to computer security.

4.3 Discussion

Eastern Illinois University has an established Computer use policy which can be viewed in detail in Appendix C or at http://www.eiu.edu/~infotech/Policy/policy.php . The information here states in part:

> Information Technology Services provides computing facilities and services for the legitimate instructional, research, and administrative computing needs of the university. Proper use of those facilities and services supports the legitimate computing activities of EIU students, faculty and staff. Proper use respects intellectual property rights.

A formal computer use policy is a necessity. Statement 11 stated:

I know the policies established by Eastern Illinois University regarding computer security and abide by them.

The responses to this statement had a mean of 3.500 and a standard deviation of 1.323 showing mixed perceptions about the established policy. The policy is established and available

on the Website. The respondents however did not appear to be substantially aware of the computer security policy.

Eastern Illinois University's computer policy states:

> Avoid accessing an account not specifically authorized to you, whether it is on an Information Technology Services system or one at another place. Avoid using an account for a purpose not authorized when the account was established, including personal and commercial use. Don't engage in computing activities that are designed to invade the security of accounts. Attempts to decipher passwords, to discover unprotected files, or to decode encrypted files are examples. (Eastern Illinois University, 1998) For a complete version of this policy see Appendix C.

Statement 18 states: *If I had the technical knowledge I would consider accessing a secure area.*

The mean for this statement was 3.105 indicating neither a strong agreement nor strong disagreement from the respondents. The standard deviation was 1.457 indicating a wide variance. The concern with this data is than some students within the SOT would consider accessing a secure area even in light of the stated policy prohibiting such access. Further education about unlawful access may be needed.

4.4 Conclusions

Eastern Illinois University has made available for students, downloads that would substantially secure a students computer in the changing world of computer malware. All this is available on the Website of Eastern Illinois University. As a result of the responses to the survey especially statement 13 which stated:

During orientation I was provided information about computer security and what Eastern Illinois University requires.

The mean for this statement was 2.227 indicating a disagreement to strong disagreement from the respondents. The perception of the respondents indicates that there may be some room for educating incoming students regarding computer security policies. Eastern Illinois University may want to consider a more prominent link to these particular pages within their website. Also statement 14 stated:

I would like more information to be provided by Eastern Illinois University about what I could do as a student to maintain a secure computer.

The mean for this statement was 3.624 indicating neither a strong agreement nor strong disagreement from the respondents. This statement regarding perceptions about Eastern Illinois University's actions while falling within the neither strongly agree nor strongly disagree range does so at the high end. The standard deviation of 1.318 indicates mixed perceptions about the amount of information provided by Eastern Illinois University. Eastern Illinois University may also consider researching a method of informing students what is available and what is required.

As a result of the survey and responses to statement 1:

I am aware that computer viruses can infect my computer in the following ways: through opening an infected email, through an infected floppy disk, through visiting an infected website.

The mean for this statement was 4.774 indicating an agreement to strong agreement from the respondents. By indicating an agreement to strong agreement to this statement students in the SOT at Eastern Illinois University appear to understand several methods of possible computer virus infection.

Then statement 5 states:

I either update my anti-virus software weekly or have the software configured to do so.

The mean for this statement was 4.278 indicating an agreement to strong agreement from the respondents. This software related statement indicates that most of the respondents do have the anti-virus on their computers set to update definitions weekly or do so manually.

Statement 8 states:

Computer viruses and worms are the only security risks I need to be concerned with.

The mean for this statement was 1.895 indicating a disagreement to strong disagreement from the respondents. The disagreement to strong disagreement to this statement indicates an awareness of threats beyond viruses.

The statement groupings provide a broader perspective of the four major areas that help answer the research question. End User Related: End user actions are a key to computer security. Statements in this grouping had the largest number of statements on the survey. Generally the responses indicated that good security practices were in place. Specifically with regard to password protection as exhibited in statements 2,3,20, and 21. Statements 17 and 18 indicated there could be some security issues from the respondents in accessing areas that were deemed to be secure. Statements 12 and 15 indicate a concern with maintaining security on their personal computer.

End User Related: Understanding is important to maintaining security. The responses of the survey indicated an excellent understanding in general as indicated by responses to statements 1,7,8,9, and 10. The responses to statements 23 and 25 even though the agree to strongly agree range, indicates a mixed perception of the respondents own understanding of computer security.

Hardware/Software related statements indicate some work is left to be accomplished as indicated by the respondent's perceptions. The use of anti-virus software and for most a firewall signifies excellent use of software/hardware and responses to statements 4, 5, and 6 indicate. The area of concern is highlighted by the responses to statements 16 and 22. These responses indicate that some have lost data and that some may be using a wireless device that may not have security features enabled.

Eastern Illinois University Related Statements indicate that many would like more information about computer security. This grouping of statements helps identify areas where Eastern Illinois University may have an influence regarding the perceptions of students in the SOT. This is highlighted by responses to statement 13. It could be that more information may not be needed but rather information on how and where to access such information. Statements 14 and 24 seem to indicate some would and some would not like more information or training in regard to computer security.

In view of the data it appears that the respondents were not fully aware of the extent of damage that many malware threats may cause. The need for further direction in accessing security measures from websites provided by Eastern Illinois University appears to indicate that the research question indicates that there is a need for continued effort in computer security. SOT students at Eastern Illinois University may have a limited understanding of the risks associated

with the use of computers and the Internet. SOT Students at Eastern Illinois University may be unaware or may fail to avail themselves of technologies which may include hardware and software available at Eastern Illinois University to reduce exposure to the risks of current technologies.

Chapter 5

Summary

This work sought to identify the perceptions of a group of those that use one such network. A survey was presented to 10 classes within the School of Technology at Eastern Illinois University. The results of this survey indicated a substantial understanding of threats posed by computer malware. The results also indicated specific use of certain software and hardware features in regard to security beyond the initial anti-virus software may need further development.

Eastern Illinois University has available for students downloads that would substantially secure a students computer in the changing world of computer malware.

As a result of the responses to the survey Eastern Illinois University may want to consider a more prominent link to these particular pages within their website. Eastern Illinois University may also consider researching a method of informing students what is available and what is required.

In view of the data it appears that the respondents were not fully aware of the extent of damage that many malware threats may cause. The need for further direction in accessing security measures from websites provided by Eastern Illinois University appears to indicate that the research question indicates that there is a need for continued effort in computer security. SOT students at Eastern Illinois University may have a limited understanding of the risks associated with the use of computers and the Internet. SOT Students at Eastern Illinois University may be unaware or may fail to avail themselves of technologies which may include hardware and software available at Eastern Illinois University to reduce exposure to the risks of current technologies.

Chapter 6

Recommendations for Future Work

This work could be furthered in a number of ways. One area of further research would be to identify the perceptions of end users for Eastern Illinois University as a whole. Furthering this research in this way would allow Eastern Illinois University to gain a broader perspective of the perceptions of the student body as a whole. This would allow the university to make choices in security measures that would be most beneficial for the student body.

A second area for further research would be to isolate the four areas that the survey statements in this work focused on and consider each in more depth. The first area being End User Related: Understanding. A closer examination of the understanding of the respondents in relation to computers and computer security should be sought. The second of the four areas to isolated would be End User Related: Actions. Actions taken by the end user play an important role in computer security. Knowing how the end user will respond enables those that have the responsibility of securing a network make better choices. A third area of the four areas to isolate would be hardware/software related. Looking closer at this area would help identify issues in the area of hardware and software. Included in this area of focus would be firewalls and email filters among other hardware devices. In this examination user friendliness or the perception of friendliness could be further researched. The fourth and final area of this section for further research would be Eastern Illinois University related. When researching the perceptions of students in this area of focus the researcher could consider what provisions are made by the university and how they are perceived. The research may extend to include possible alternative measure to dispense provision made for computer security by the university.

A third area for further research may be to follow a class from entering Eastern Illinois University through graduation. This research may examine changes in perception of the student. Research questions may include. Does the perception of the student change as the student becomes more familiar with the university? Does implementation of further security measures create the perception of a secure network or is it received as a restrictive nuisance?

A fourth area for further research may be to expand research to include the perceptions of end users in all State Universities in Illinois. This examination of different universities may offer insights about how students perceive security in different situations. Possible outcomes may include identifying methods of security that are better received than others.

References

Audin, G. (2004, June). Next-Gen firewalls: What to expect. *Business Communications Review, 34*, 56-61. Retrieved February 10,2005, http://proxy.library.eiu.edu:2068/WebZ/FSFETCH?fetchtype=fullrecord:sessionid=sp07sw05-64394-e5fqmx31-st0xtf:entitypagenum=3:0:recno=1:resultset=1:format=FI:next=html/record.html:bad=error/badfetch.html:entitytoprecno=1:entitycurrecno=1:numrecs=1

Barracuda networks (2005). *Website.* Retrieved November 8, 2005, http://www.barracudanetworks.ca/faqs.htm

Eastern Illinois University, (2005, July 21, 2005). *Cisco Clean Access.* Retrieved November 7, 2005, http://mypc.eiu.edu/cca/

Eastern Illinois University, (1998, February 4). *Statement of Eastern Illinois University Policy Use of Network Facilities and Services Including World Wide Web.* Retrieved November 8, 2005, http://www.eiu.edu/~infotech/Policy/policy.php

Foster, A. L. (2004, March 19). Colleges Brace for the Next Worm. *Chronicle of Higher Education, 50*(28), 29-31.

Furnell, S. (2005, June). Why users cannot use security. *Computers 7 Security, 24*(4), 274-279.

Grimes, R. (2005, September 26). Are Attackers Winning the Arms Race? *InfoWorld, 27*(39), 23-29.

Hayes, F. (2003, July 14, 2003). The Story So Far. *Computerworld, 37*, 26. Retrieved February 20, 2005, http://proxy.library.eiu.edu:2068/WebZ/FSEmail?sessionid=sp07sw05-64394-e5fqmx31- st0xtf:entitypagenum=103:0:entityemailfrom=ftascii:entityemailrecno= 56: entityemailresultset=8:entityemailnumrecs=1

Hulme, G. (2004, December 6, 2004). New Threats Ahead. *InformationWeek, 1017*, 67. Retrieved February 20, 2005, http://proxy.library.eiu.edu:2068/WebZ/FSEmail?sessionid=sp07sw05-64394-e5fqmx31-st0xtf:entitypagenum=36:0:entityemailfrom=ftascii:entityemailrecno=2:entityemailresultset=8:entityemailnumrecs=1

Karabacak, B. & Sogukpinar, I. (2005, March). ISRAM: information security risk analysis method. *Computers & Security, 24*(2), 147-159.

Krazit, T. (2005, June 17, 2005). *Security breach may have exposed 40M credit cards.* Retrieved September 25, 2005, http://www.computerworld.com/securitytopics/security/story/0,10801,102631,00.html?from=story_picks

Maggiora, P. D., & Doherty, J. (2003). *Cisco Networking Simplified.* Indianapolis, In: Cisco Press.

Miastkowski, S. (2001, November). Symantec Utilities: Worth the Upgrade. *PC World, 19*, 68-69. Retrieved February 23, 2005, http://proxy.library.eiu.edu:2068/WebZ/FTFETCH?sessionid=sp07sw05-64394-e5fqmx31-st0xtf:entitypagenum=149:0:rule=100:fetchtype=fulltext:dbname=WilsonSelectPlus_FT:recno=44:resultset=20:ftformat=PDF:format=BI:isbillable=TRUE:numrecs=1:isdirectarticle=FALSE:entityemailfullrecno=44:entityemailfullresultset=20:entityemailftfrom=WilsonSelectPlus_FT:

Ozkan, B. C., & Gunay, V. (2004, August). Minimizing Security Vulnerabilities in High Tech Classrooms. *T.H.E. Journal, 32*(1), 32-36.

Phelps, E. F. (1997, December). Securing a plan. *American School & University, 70,* 50-52.

Postini Integrated Message Management (2005). *Postini Resource Center.* Retrieved 11-27-05, http://www.postini.com/stats/

Rist, O. & Rash, W. (2003, August 11). Firewall Free for All. *InfoWorld, 25*, 37-45. Retrieved February 18, 2005, http://proxy.library.eiu.edu:2068/WebZ/FSQUERY?sessionid=sp07sw05-64394-e5fqmx31-st0xtf:entitypagenum=93:0:numrecs=1:searchtype=locateFT:tdbname=WilsonSelectPlus_FT:query0=sc%3d%220199-6649+20030811+25+31+36+FF+%3F%22:format=BI:entityfttoprecno=51:next=NEXTCMD%7FFTFETCH:rule=0:tdbname=WilsonSelectPlus_FT:issuesici=0199-6649+2003+25+31:fetchtype=fulltext:tdisplaydbname=WilsonSelectPlus_FT:thirdpartydbid=8:isbillable=TRUE:isdirectarticle=FALSE:numrecs=1:format=BI:ftformat=PDF:entityemailfullrecno=51:entityrecno=51:entityemailfullresultset=8:entityemailftfrom=WilsonSelectPlus_FT:%7F

Stanton, J. M., Stam, K. R., Mastrangelo, P. & Jolton, J. (2005, March). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

Symantec (2005). *Symantec Products and Services.* Retrieved 11-27-05, http://www.symantec.com/product/index.html

Vijayan, J. (2005, June 30, 2005). *Credit card data security standard goes into effect* . Retrieved September 25, 2005, http://www.computerworld.com/securitytopics/security/story/0,10801,102913,00.html

Wikipedia, (). *Internet bot.* Retrieved October 13, 2005, http://en.wikipedia.org/wiki/Internet_bot

Wilson, J. (2005, May). The Future of the Firewall. *Business Communications Review,* (5), 28-32.

Appendixes

Appendix A

David C Fulton
Computer Security Survey
Fall 2005

Phone: 217-621-3409
Fax:
E-mail: d-fulton@sbcglobal.net

Effectively Securing Your Student Computer: A Security Survey

This survey is being used to collect data for use in the preparation of my thesis. This survey is designed to assess security issues related to college students. It will try to determine security practices and concerns related to you as a student. The data will be calculated as a class and no individual names will be used so please answer as honestly and freely as you can. Please answer the following questions using the scale at the right. Please circle your answer with 1 being strongly disagree and with 5 being strongly agree.

Strongly Disagree **1 2 3 4 5** Strongly Agree

1.	I am aware that computer viruses can infect my computer in the following ways: through opening an infected email, through an infected floppy disk, through visiting an infected website.	1 2 3 4 5
2.	I always protect my user passwords for my computer and any computer accounts I may have access to.	1 2 3 4 5
3.	I never share my password with my friends or associates.	1 2 3 4 5
4.	I have an anti-virus software installed on my computer.	1 2 3 4 5
5.	I either update my anti-virus software weekly or have the software configured to do so.	1 2 3 4 5
6.	I use a firewall on my personal computer.	1 2 3 4 5
7.	If I have an anti-virus software I am guaranteed to not be infected by a virus.	1 2 3 4 5
8.	Computer viruses and worms are the only security risks I need to be concerned with.	1 2 3 4 5
9.	It is possible for my computer to be infected and I would not realize it.	1 2 3 4 5
10.	I understand that new viruses and worms may reside dormant until a later time.	1 2 3 4 5
11.	I know the policies established by Eastern Illinois University regarding computer security and abide by them.	1 2 3 4 5
12.	I use security measures made available by Eastern Illinois University.	1 2 3 4 5
13.	During orientation I was provided information about computer security and what Eastern Illinois University requires.	1 2 3 4 5

David C Fulton
Computer Security Survey
Fall 2005

Phone: 217-621-3409
Fax:
E-mail: d-fulton@sbcglobal.net

Effectively Securing Your Student Computer: A Security Survey

14.	I would like more information to be provided by Eastern Illinois University about what I could do as a student to maintain a secure computer.	1 2 3 4 5
15.	If I were provided software by the university I would install and keep the software updated.	1 2 3 4 5
16.	I have lost data of some form due to a computer virus or a security breach.	1 2 3 4 5
17.	I have never tried to access a secure area on a network.	1 2 3 4 5
18.	If I had the technical knowledge I would consider accessing a secure area.	1 2 3 4 5
19.	I have unknowingly accessed a secure area on a network.	1 2 3 4 5
20.	I have received the password of a classmate, co-worker, or associate.	1 2 3 4 5
21.	If I received a phone call from someone claiming to be from Eastern Illinois Universities IT department I would give them my password if requested.	1 2 3 4 5
22.	My wireless router is properly configured to prevent access by unauthorized persons. If you do not have a wireless router please leave blank.	1 2 3 4 5
23.	I have a good understanding of computer security and measures needed to protect my computer and data.	1 2 3 4 5
24.	I would like to receive additional training in regard to computer security and resources available from Eastern Illinois University.	1 2 3 4 5
25.	Rate your level of computer technical expertise where 5 is high level of expertise and 1 is a low level of technical expertise.	1 2 3 4 5

Appendix B

Eastern Illinois University also has implemented a service called Cisco Clean Access See Figure 1 Clean Access Agent Website

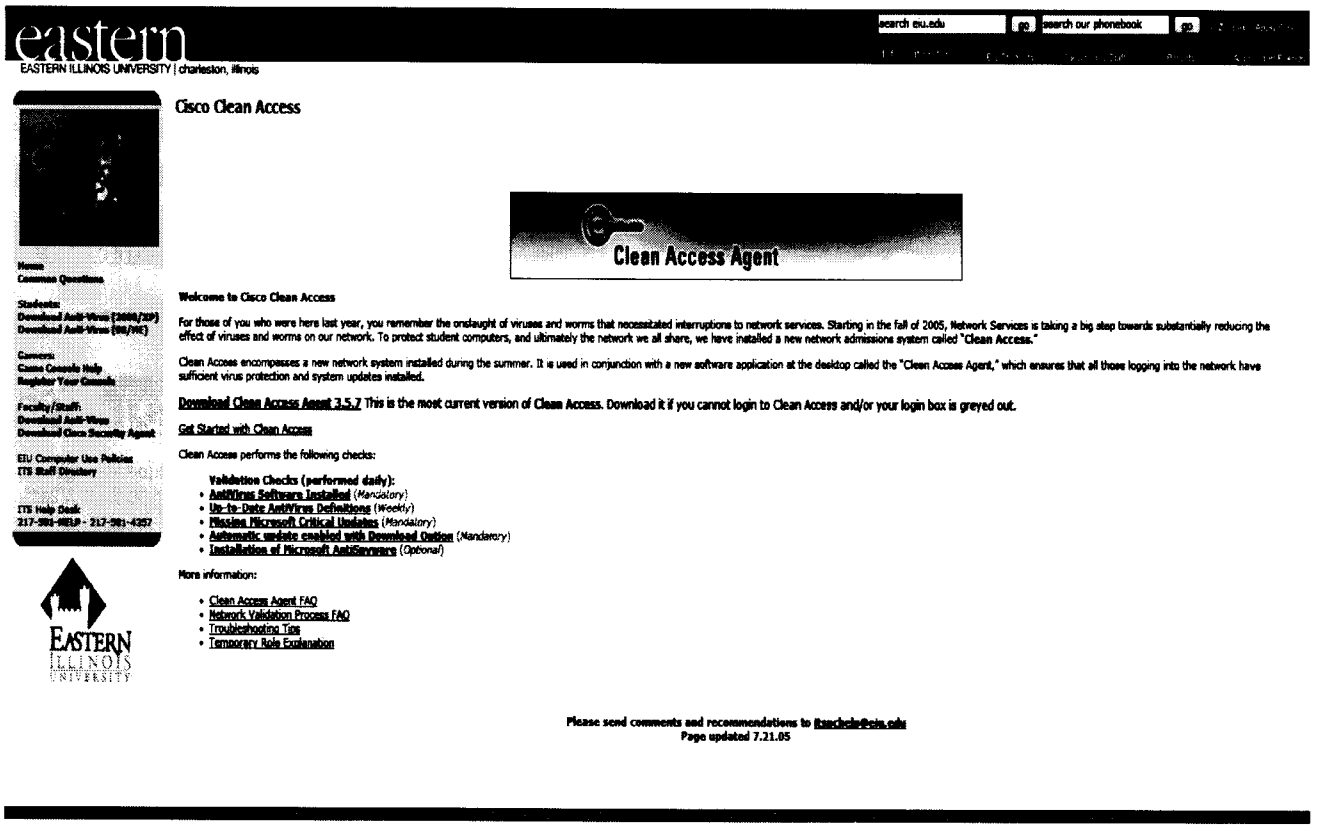


Figure 1 http://mypc.eiu.edu/cca/ (Eastern Illinois University, 2005).

This site explains the Clean Access Agent and the purpose this service provides. This software basically ensures that computers logging onto the Universities network has antivirus software and that the computer has the latest antivirus definitions. The software also checks the computer attempting to connect to the network for Microsoft critical updates and that automatic updates is enabled. Users are required to log in to the network at specified maximum intervals to allow these checks to take place.

In the discussion regarding Eastern Illinois Related statements the conclusion generally stated that many students within the SOT more information about the provisions that are made

by eastern Illinois University. This Website and the available information with links would provide SOT students substantial information to get started. If this were somehow made more prominent SOT students would be introduced too much needed information.

Eastern Illinois University also has a site available for a student to download available software needed to satisfy most of the Clean Access Agent requirements. Otherwise Clean access Agent directs the student where to obtain the needed updates. This download site is http://mypc.eiu.edu/ .

Figure 2 Eastern Illinois University Student Software Download Site

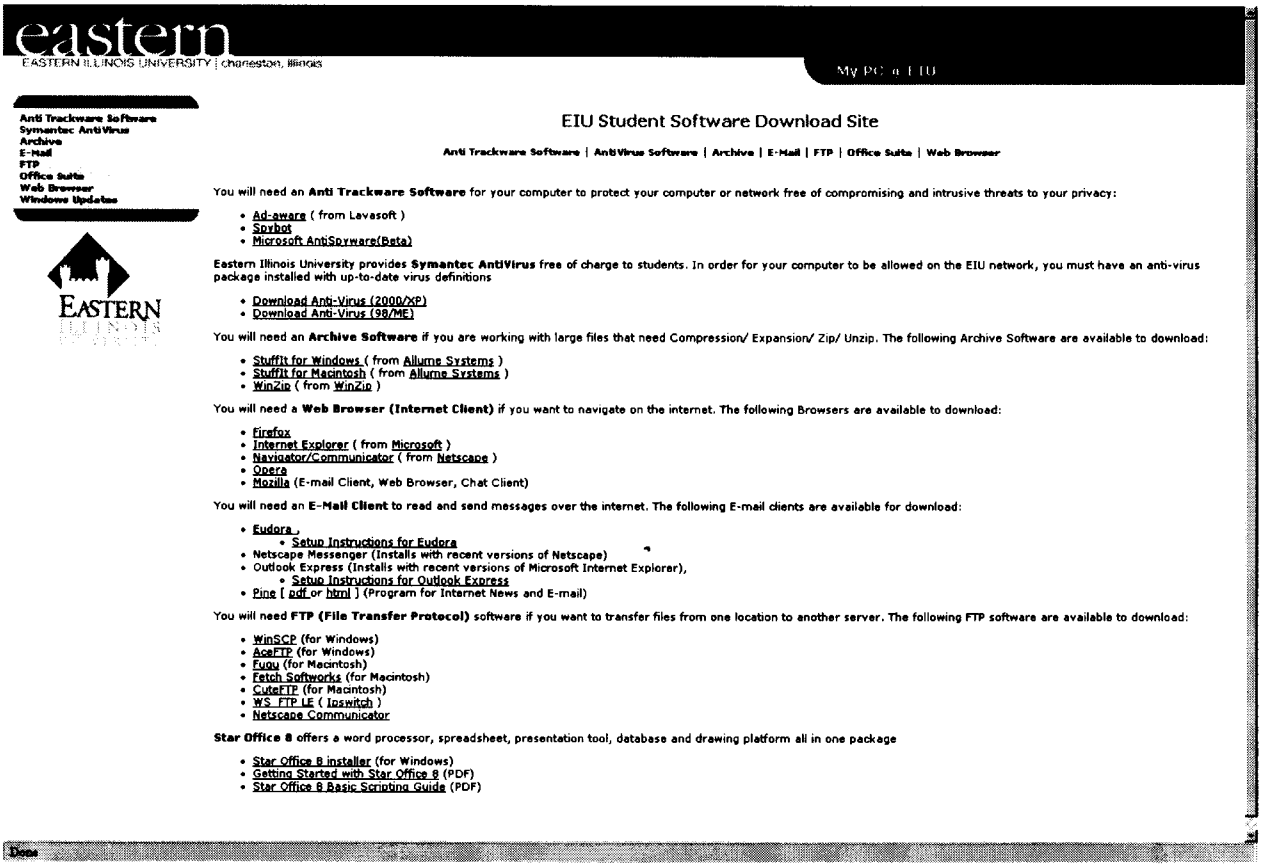


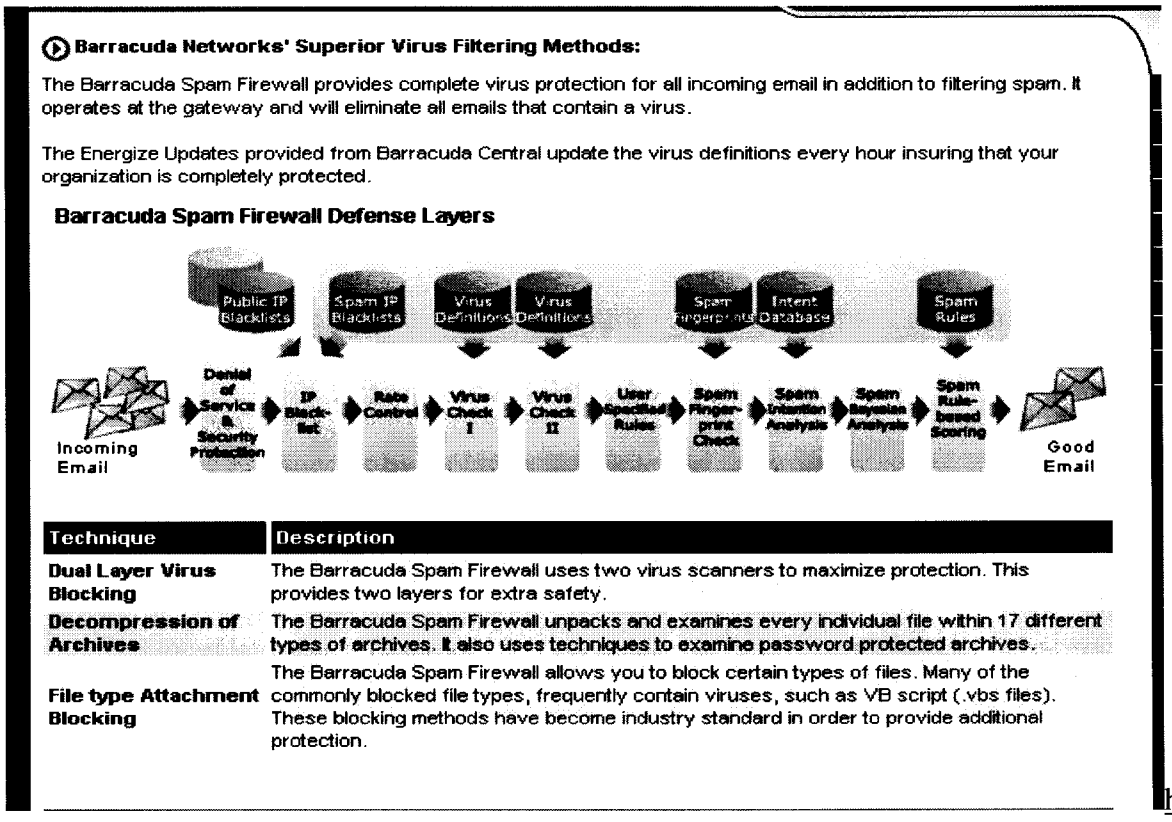
Figure 2 http://mypc.eiu.edu/ (Eastern Illinois University, 2005).

This software download Website provides the means for students at Eastern Illinois University to be using their computer in a secure environment. The data indicated that many

students within the SOT programs have security software installed on their computers. By providing the software and this download Site Eastern Illinois University is proactively assisting their students with security measures. By promoting this area of the school's Website the school could further enhance the perception of students in the computer security area.

Further Eastern Illinois University has implemented an email spam filter to further eliminate spam and potential virus infections. The school has employed a hardware device called Barracuda, which is a physical device that serves as a spam filter and an additional layer of virus protection (Barracuda networks, 2005). This device is an additional layer of security that provides a much needed service since many emails are used to spread viruses. Figure 4-3 shows how this filter works.

Figure 3 How is Spam Filtered?



http://www.barracudanetworks.ca/faqs.htm Question 14 (Barracuda networks, 2005)

Appendix C

Statement of Eastern Illinois University Policy Use of Network Facilities and Services Including World Wide Web (WWW)

Information Technology Services provides computing facilities and services for the legitimate instructional, research, and administrative computing needs of the university. Proper use of those facilities and services supports the legitimate computing activities of EIU students, faculty and staff. Proper use respects intellectual property rights.

Legitimate instructional computing is work done by an officially registered student, faculty, or staff member in direct or indirect support of a recognized course of study. Legitimate research computing is work approved by an authorized official of a university department. Legitimate administrative computing is work performed to carry out official university business.

Intellectual property rights begin with respect for intellectual labor and creativity. They include the right to acknowledgment, the right to privacy, and the right to determine the form, manner and terms of publication and distribution.

Proper computing use follows the same standards of common sense and courtesy that govern use of other public facilities. Improper use violates those standards by preventing others from accessing public facilities or by violating their intellectual property rights. Therefore, the basic policy of the university on proper use is:

- Any use of Information Technology Services facilities or services unrelated to legitimate instructional or research computing is improper if it interferes with another's legitimate instructional or research computing.
- Any use of Information Technology Services facilities or services that violates another person's intellectual property rights is improper.

- Any use of Information Technology Services facilities or services that violates any university policy, any local, state or federal law, or which is obscene or defamatory is improper.
- Any use resulting in commercial gain or private profit (other than allowable under university intellectual property policies) is improper.

The following sections describe some known instances of improper use. They do not constitute a complete list. When new occasions of improper use arise, they will be judged and regulated by the basic policy stated above.

Disruptive Conduct

Avoid behavior at any computing facility that would interfere with another person's legitimate use of the facility. This includes noisy and over-exuberant conduct.

Damage

Avoid actions that would damage Information Technology Services facilities, hardware software, or files.

Access to Files

Avoid reading or using others' files without their permission. Proper usage standards require everyone to take prudent and reasonable steps to limit access to their files and accounts.

Fraud and Forgery

Avoid sending any form of electronic communication that bears a fraudulent origin or identification. This includes the forging of another's identity on electronic mail or news postings.

Copyright

Refer to Eastern Illinois University Regulation 16a.and applicable sections of the Federal Copyright Act, including fair use provisions I Section 107 of H.R. 2223, to avoid violating the copyright law as you contemplate copying software, digital images, and other electronic media. You should also review the report of the Information Infrastructure Task Force (IITF) for concerns about digital images and educational multimedia.

Harassment

Avoid using the university computing facilities to harass anyone. This includes the use of insulting, obscene or suggestive electronic mail or news, tampering with others' files, and invasive access to others' equipment.

Networks

Avoid using local, national and international networks for things that are not legitimate instructional or research activities of the university. This includes, but is not limited to articles for commercial gain posted on electronic news networks and repeated attempts to access restricted resources.

Unauthorized Use of Accounts

Avoid accessing an account not specifically authorized to you, whether it is on an Information Technology Services system or one at another place. Avoid using an account for a purpose not authorized when the account was established, including personal and commercial use.

Don't engage in computing activities that are designed to invade the security of accounts. Attempts to decipher passwords, to discover unprotected files, or to decode encrypted files are examples.

Proper usage standards require that everyone take prudent and reasonable steps to prevent unauthorized access.

Unauthorized Use of Software

Do not make unauthorized copies of licensed or copyrighted software. Do not make copyrighted or licensed material accessible from a Web page without the specific written permission of the copyright owner.

Avoid actions that are in violation of the terms or restrictions on the use of software defined in official agreements between the university and other parties.

Examples include: the copying of software from personal computers unless it is clearly and specifically identified as public domain software or shareware that may be freely redistributed; and the copying of restricted UNIX source code. Read the policy topic "Rules for Access to UNIX Source Code" for more information on UNIX license restrictions.

WWW Specific Clauses

General policies for computer use apply to those who develop or are responsible for the development of web pages on our World Wide Web server. However, the ability to publish electronically creates some unique opportunities and concerns.

1. **Privacy**

   People have a right to privacy. Employees acting within the scope of their employment may not place any item(s) (regardless of whether the person can be identified) such as, but not limited to, pictures, videos, audio-clips, or information about an individual(s) without the express written permission of the individual(s). The exception is those items that are determined to be necessary for university administrative functions.

2. **Fair Warning**

   Users of the EIU WWW must realize material put on the WWW is available to a wide audience, often beyond that originally intended for the material. There must be a recognition that, in different contexts, material may be construed in a manner different from that of the original intention of the author(s). Therefore, at the request of the appropriate university official(s), an information provider will provide a warning page at one level before any WWW page(s). This will be a standard page expressing that the content below may not be suitable for all audiences. WWW users, particularly minors, have a right to a "fair warning."

3. **Use of University Name, Seal, and Logo**

   Use of the university name, seal, and logo is not permitted except as allowed and/or required by university policy and regulations.

4. **Personal Home Pages and WWW Servers**

   EIU provides Internet/WWW access and resources for conduct of university functions. Personal use, e.g. development and posting of personal home pages and WWW servers, is permitted insofar as such activity does not disrupt, due to time, place, or manner, the conduct of university functions and as long as it is in compliance with the remainder of this and other university policies. The official EIU home page will not link directly to personal pages

Enforcement

When instances of improper use come to its attention, Information Technology Services will investigate them. During those investigations Information Technology Services reserves the right

to access private information, including the contents of files and mailboxes, while making every effort to maintain privacy. Investigations that discover improper use may cause Information Technology Services to:

- Limit the access of those found using facilities or services improperly;
- Refer flagrant abuses to deans, department heads, the responsible vice president, the university flagrant abuses to deans, department heads, the responsible vice president, the university police, or other authorities for appropriate action;
- Disclose private information to other university authorities.

Users who violate this policy may have their computing privileges terminated and may be subject to disciplinary action by the university in accordance with appropriate policies or judicial affairs procedures.

Rules for Access to UNIX Source Code and Licensed Software

One of the big factors in the increasing popularity of the UNIX operating system at EIU is how easily UNIX source code applications can be moved among different variations of the UNIX system. This process, commonly called porting, often requires nothing more than copying and compiling an application to move it from one UNIX platform to another. The porting process is so simple that it is easy to lose sight of the ownership of individual programs and the license agreement restrictions on their source code.

1. **License Agreements**

   Source code for computer programs is usually owned by the organization that developed the programs. Since many of these organizations have an economic stake in their

developmental investment, they don't just give it away. At a minimum, they usually declare their copyright on the programs. But legally, a more powerful means exists: a license agreement.

Software license agreements are contracts in which the seller agrees to provide the program, and perhaps its source code, provided that the buyer agrees to abide by the rules of the license. Most workstation-based software that is issued with the installation of a UCAN workstation is licensed software. NCSA Telnet and Kermit packages are noted exceptions. Sellers can specify just about any rules they desire so long as the buyer agrees to those rules. And just to make life interesting, every seller of computer software seems to have its own special rules to follow. Licensed software must not be duplicated, distributed, modified, or used without authorization.

Some programs are distributed in source form without a license agreement. They may be totally unrestricted (called ``public domain'') or the owner may retain the copyright but allow free distribution. A lot of useful software designed to run on UNIX systems is distributed this way. As a user of one of EIU's systems, you may find source code to such programs in various system directories.

2. **Source Code at EIU**

Whenever possible, most UNIX system administrators at EIU strive to obtain the source code for programs because it makes it easier to maintain systems and quickly fix problems. In order to obtain source code for commercial software systems, it is necessary to negotiate the ``Terms and Conditions'' of the software license agreement with each software vendor. Some of those agreements permit anyone at EIU to have access to the

source code while others stipulate restrictions. Therefore, you may find that you have access to source a source code that is restricted by a license agreement. Just because you have access does not mean you have the right to port a program to another system.

When it comes to the UNIX operating system and its associated utilities and libraries, EIU adheres to license agreements with IBM, Sun Microsystems, the University of California at Berkeley, and other vendors that redistribute UNIX. These license agreements specify the rules under which we may have access to the source code in the first place.

If you have a **UNIX system** of any kind and want to obtain source access, please follow these rules:

- Check with the source-code vendor to determine if an additional vendor license is required. Follow the vendor's restrictions on redistributing the vendor's source code.
- Source code access for most Sun UNIX systems is provided under agreements between EIU and the Sun Corporation.
- When in doubt, do not assume you have the right to copy sources from another UNIX system to your own; contact the SUN license administrator at EIU or the administrator of the system from which you wish to copy the sources before doing so.

Waste

Avoid any wasteful use of Information Technology Services facilities. This includes squandering expendable resources, processor cycles, disk space, or network bandwidth. Use expendable resources such as paper prudently, and recycle them if possible. Use a system whose capacity is appropriate to the size of the computing task.

Requests for Services

Information Technology Services is the central coordinating department for computerized instruction, research, and administrative functions of the university. If a change in or addition to programming or networking services is desired, a request must be submitted, in writing, to the Associate Vice President for Information Technology Services. The request shall state in detail the change in service desired and shall be signed by the Fiscal Agent of the requesting unit. User Services support requests should be brought to the attention of the Director of User Services, or if clarification is needed, the request should be discussed with a member of the staff within the User Services Division of Information Technology Services.

Information Technology Services staff shall not be responsible for initiating changes in administrative mainframe applications; however, they do maintain the right to make suggestions. Applications shall be revised when systems software requires it or when hardware that is necessary for processing reaches obsolescence.

Acquisition of Commodities

The Information Technology Services operations manager maintains the inventory of supplies necessary for central data processing system operation. The acquisition of microcomputer supplies is the responsibility of the owning department. Forms that are currently not on inventory must be acquired by the requesting department. However, the acquisition of new forms to be printed by mainframe connected printers must be coordinated through the Associate Vice President of Information Technology Services or the Assistant Director for Operations.

Microcomputer and Network Services

Information Technology Services shall provide the following services:

1. **Maintenance**

   Services provided by Information Technology Services staff shall include the repair of microcomputers that are currently approved for maintenance support and consultation on microcomputer and software purchases. Replacement parts are a part of this service fee; however, if, in the judgment of the Information Technology Services staff, the microcomputer is beyond repair, the using department shall be responsible for funding any replacement. A maintenance service fee shall be charged for each IBM PC/XT/AT, Zenith, Swan, Apple, or other covered microcomputer that was purchased from an account other than an appropriated account and that is on inventory.

2. **Network Support Services -- Uniform Campus-wide Area Network (UCAN)**

   Information Technology Services staff shall provide for the installation of network hardware and software components and shall service the communications components that are installed by them. The UCAN circuit boards and the electronic equipment within wiring closets is to be maintained and modified by Information Technology Services staff only. UCAN software components should all be treated as licensed software by end users.

Printers, Plotters and Modems

Information Technology Services staff shall provide advice and minor repairs for printers, plotters and modems; however, the using department is responsible for major repairs and replacements. Examples of minor repairs would include cleaning, simple mechanical adjustment, and the replacement of a print head that is furnished by the using department.

Mainframe, UCAN Network Server, and Work-station File Security

Information Technology Services acts as the custodian of all university data bases or data processing files, but it is not the owner of these files. Individual users should take reasonable precautions regarding the physical security of their equipment and should change their passwords frequently. The system administrator for servers other than the mainframe will provide mechanisms for backup and password controls. However, the management, security, and backup of files stored on servers other than the campus mainframe are the responsibility of the individual user. You are best able to assess the level of privacy and security of the data and text files that you create.

Approved:

President's Council

February 4, 1998