ED 405 808 IR 018 248

AUTHOR Anderson, John A.

TITLE Ethics, Privacy, and Security in Higher Education Technology.

PUB DATE 96

NOTE 9p.; In: Association of Small Computer Users in Education (ASCUE) Summer Conference Proceedings (29th, North Myrtle Beach, SC, June 9-13, 1996); see IR 018 247.

PUB TYPE Reports - Evaluative/Feasibility (142) -- Speeches/Conference Papers (150)

EDRS PRICE MF01/PC01 Plus Postage.

DESCRIPTORS Codes of Ethics; Computer Networks; *Computer Security; Confidentiality; *Crime Prevention; *Employee Responsibility; Higher Education; Information Policy; *Information Technology; Internet; *Privacy; School Security; Technological Advancement; Users (Information)

IDENTIFIERS *Computer Ethics; *Data Security; Family Educational Rights and Privacy Act 1974

ABSTRACT

Information Technology (IT) personnel in higher education requirement at Mary Washington College, Virginia. The goal of the creativity, promote freedom of speech, support research and investigation, and provide information access globally, while demonstrating proper use and protection of the data of which they are in charge. This paper addresses issues of ethics, technology crimes, security, and privacy, and provides recommendations for improving protection of critical information on campus computer systems. IT personnel deal with security and privacy issues from a technical standpoint and are not sufficiently trained to deal with the social ramifications of these issues from a non-technical viewpoint. In addition, high tech codes of ethics and laws are basically non-existent and current laws are both outdated and do not have provisions for the new technologies. Ethics is a gray area that deals with actions that are not technically illegal, but are not quite right, either. Technology has both de-personalized crime and created new opportunities for crime. IT personnel must commit more resources for security development, comply with the Family Educational Rights and Privacy Act at a minimum, encourage ethical behavior, and "proper use" policies with all user communities, and keep aware of developments in the technology world. (Author/SWC)

Ethics, Privacy, and Security in Higher Education Technology

John A. Anderson
Director of Information Services
Loras College
Dubuque, IA 52001
hawks@lcac1.loras.edu

You read about it every day. Technology progress continues at a frightening pace and more and more of our society seem to be dedicated to negate all of the positive aspects that technology brings to improve our life styles. For many years now, the computer has been blamed for most headaches and mistakes that are by-products of the computerization of America. Let's face it, some people just love to hate technology. For years, technology professionals have explained that computers can only do what they are programmed to do, but in spite of this effort, the reputation has developed that all technology is unpredictable, insecure, and unreliable and therefore is just one more thing to avoid.

Technology has both benefits and drawbacks, but it must remain clear that computers are only the tools, and the way that society utilizes these devices is the actual source of the problems. The computer has done nothing more than create new versions of old moral issues like honesty, right and wrong, responsibility, confidentiality, fairness, and loyalty. The misuse of computers by humans only adds fuel to the flames. This misuse comes in many flavors and includes:

- unauthorized access
- theft of money, software, information, etc.
- disputed rights to data and products
- use of computers for fraud
- hacking and virus creation
- degradation of work

Many of these are criminal behavior and some are ethical issues, but regardless of their classification they are tremendous problems for technology professionals in institutions of higher learning. These problems do not stop with data, but have expanded into the voice and video areas. In some cases, higher education institutions are being blamed for providing the know-how and the facilities that are the heart of improper use of technology.

Our responsibility in Information Technology is to encourage constructive creativity, promote freedom of speech, support research and investigation, and provide information access globally, while demonstrating proper use and protection of the data that we are placed in charge of. The speed with which the technology field has progressed on college campuses and the general lack of understanding surrounding most technology has created a monster with more power than any college administrator could ever believe. Information Technology personnel, however, have all this power that they never really asked for. Unfortunately they are technical people and are not sociologists or guidance counselors that they are being asked to be. They deal with security and privacy issues from a technical standpoint and are not sufficiently trained to deal with them and their social ramifications from a non-technical viewpoint. To complicate matters worse, high tech codes of ethics and laws are basically non-existent and current laws are both outdated and confusing since they were not written to deal with the technologies of today.

As an Administrative Computing director at my institution for the last 18 years, I have read and observed wave after wave of security problems on computer systems and networks. Not being connected to a campus-wide network or to the academic computer system has provided me the luxury of sitting back and being an observer rather than a worrier. Of course we had one dial-up modem that was a worry, but I could just unplug it when the stress builds up and plug it back in when I regained courage. Now they tell me that I should attach my fairly secure system to the campus-wide network, and as if that wasn't enough, they actually want me to allow access for faculty and students to my administrative database information. This will obviously add to my concerns about security and privacy of information.

I feel lucky that I haven't needed to be concerned with these potential problems and was able to concentrate on the more productive mission of providing maximum and quality information for my administrative users. I believe the complexity of administrative software and continuous revisions to keep current with ever-changing requirements was more than enough to keep our staff busy. Connectivity means that we must now commit some additional attention to protecting data from external users, authorized or unauthorized. This, of course, is in addition to the additional requirements placed on us with learning, developing, implementing, monitoring, and maintaining networks.

Ethics

Ethics is that gray area that deals with things that are done using computers that aren't quite illegal, but aren't quite right, either. I'm not going to attempt to categorize every situation into an ethical or legal issue. I'm neither an attorney nor a fortune-teller. The problem with trying to label different issues is that there are insufficient laws or rules to cover most technical issues and there aren't even adequate definitions to use in identifying the seriousness of each issue. Fed by the complexity of current systems and networks, ethics are usually not in the minds of users as they log in. I believe that there is so much information available to Internet users, that we have totally lost the value of private, secure information. Most hardware and software companies are introducing products faster than the quality control people can verify security weaknesses and the products are installed in our colleges much quicker than we can adequately test for loopholes. As end-users become more independent, they load their own software and wander where ever they want in cyberspace, creating an ever-present awareness by data managers that they are no longer in control of anything.

As management of this technology we are advising, counseling, and providing liaison roles in ethical and legal situations on our campuses. Many times the technical staff make judgements about what is legal and not legal to do on a computer system with little knowledge of what is result of their judgement. This places technical people in a role they were not trained for and usually that they don't want. I know that I find myself, in many instances, defending how we do things to upper-level management as well as the end-user that has become a victim of improper use of resources. The lack of established and clear laws, codes of ethics, policies, and penalties, has made this aspect of our positions one of the most troublesome.

Some typical questions that complicate the assessment of proper technical usage are:

- Who really owns the data stored on computer files?
- What if the data is about you?
- If an unauthorized person breaks into a system and just looks at your information without altering it, is that illegal? unethical?
- What information can be public? What can't be public? Who should control release of this information?
- When does personal use of technology become excessive or criminal?
- Breaking into a system really breaks nothing, so is this a crime if nothing is altered?
- Who determines when content is offensive to others? What constitutes harassment? How far does freedom of speech go?
- Should it be a crime to share hacked information on public electronic bulletin boards?

This list is far from complete, but it is pretty obvious that everyone has their own opinion about these issues and they usually go so far as to state that there are right and wrong answers to each. This is the precise reason that it is not easy to pin down right from wrong or ethical from illegal. The only thing that is clear to me, is that current technology levels are allowing users to stretch ethical behavior to the limit.

I believe that the information revolution that we have been experiencing has simply provided the opportunity for usually honest people to become criminals. This opportunity has provided a severe temptation to abuse money and power through technology. I feel though that hacking systems is quickly replacing baseball as the number one American pastime and that money and power aren't always the motive. Sometimes the reason for this behavior is simply for entertainment. We have seen all types of media sensationalize the "nerd" stereotype. No wonder some socially inept people might identify with this image and seek to form relationships using the remote and abstract interaction of network computing. Some people just are seeking the intellectual challenge of "beating" a computer or are substituting the undemanding computer relationship for real-life one-on-one relationships with people.

Many times the computer abuse just begins with doing the local mailing list for the local theatre group. Then someone else calls and asks if they can purchase a list of all students and employees on the campus. Before anyone realizes, money is changing hands and the college computer is being utilized for so many off-campus services that our own database information can't be retrieved in a timely manner. When does enough become too much. This is a hard thing to decide and control. When there is financial gain involved, the issue becomes clearer to decide. When issues of this nature occur, it is very difficult to resolve the problem without bad feelings, so usually management turns their heads and ignores the activity. This doesn't help either party, since it sends a message that this "stealing" of resources is acceptable, even though this is not really the management position on the matter.

This personal use leads to other types of resource abuse. The excessive use of resources can involve processing time, computer paper, and access time. Many times game playing on computers is a huge problem in lab settings. But with the introduction of e-mail and World Wide Web access to the desktop, a new level of abuse corrodes the concept of staff productivity in the workplace. Supervisors now need to struggle with the balance of using WWW as a creative tool to enhance functionality against the wasted time of employees searching endlessly for non-relevant information and trading personal e-mail with friends at other institutions.

The whole area of "freedom of speech" is an ethical nightmare with internet access for everyone. There have been recent laws attempting to control pornographic content on public networks, along with limits on sexual, political, and racial harassment using technology. This is just the beginning. The problem with most of this "small-time" crime, is that most people that are caught, don't even consider their "crime" to be unethical or dishonest.

Earlier I posed the question about whether it was illegal or unethical to simply look at secured data. It is clearly wrong to delete or alter data once a security breach occurs. But what if the person just "looks around" and harms nothing. Like we said, a breakin actually breaks nothing, only security is compromised. If files are copied, the original is left intact. Has any harm occurred other than the hacker did something that they weren't supposed to? The factors at work here are probably the sensitivity and importance of the information, the disposition of the copied software, whether the action was pre-meditated and malicious, and was any damage that occurred intentional or accidental.

Another war that is surfacing as an ethical issue is the battle between social responsibility and intellectual rights. Some users view hacking as intellectual exploration while system administrators see the intruders as criminals. This activity is sometimes ignored, but when networks are disabled or files are altered or deleted this becomes an issue with the same people that viewed it previously as harmless. Some institutions are going to the extent of hiring student hackers to legally attempt to breach their system's security to discover weaknesses and loopholes. Does this make good sense?

Unauthorized access is a game to many hackers and has spread to stealing cable television, free long-distance telephone calls, cellular fraud, video piracy, and reprogramming of computerized devices in the community (traffic lights, elevators, etc.) The realization by technical staff of an institution that they have had a breach of security is the first major step. Acknowledgement of the situation, however, is not that easy. Most institutions are very reluctant to admit vulnerability of their systems. It would be an admission of negligence and reflects negatively on the image and trust of the institution within the community. At these times of extreme competition for recruiting students and being involved in the community, it could be disastrous for an institution to lose public confidence.

Crimes and Technology

Technology has created opportunities for crime that didn't exist even a few years ago. The technology of crime detection grows almost as fast as the computer related crimes, themselves. The scariest factor of all, is that most computer crime is discovered by accident. So how much goes undetected? It is so difficult to monitor how bad this situation is when nobody wants to admit to being a victim.

With some technology-related crimes there is no ethical dilemma. Theft of money, information, or services and the alteration and destruction of information should be considered crimes. What makes this so difficult is that society has a hard time determining these actions as criminal because there usually is no physical evidence of destruction. Without the physical nature of technology crimes the offense doesn't seem quite so bad.

What has happened is that computers have de-personalized crime. Most technology abuses are victim-less or at least the real victim is unclear. Because of this, the person committing the crime, doesn't feel like they have really hurt anyone and most times don't really think about the effect of what they have done. When an individual creates and distributes a virus that destroys the boot portion of a disk, they are harming people that they don't even know. With networking of systems we have created the opportunity for criminal acts with very little, if any, risk. Also, most crimes committed using technology are accomplished by an individual. This further decreases the risk of getting caught, because there are no accomplices. In most cases, the best security is no match for the persistence and patience displayed by most criminals. Constantly the criminal computer user learns how to use technology to combat the technical-based security that has been created to attempt to keep them out.

Security

We work with four categories of security in technology; hardware, software, network, and physical. Depending on your particular setup on your campus you have varying degrees of security at each of these levels. Typical methods are passwording, encryption, virus detection, dial-back modems, authorization lists and firewalls. While this seems like a fair amount of tools to combat the unauthorized hits on our systems and networks, these are a pitiful arsenal of defenses to use against the growing number of hackers in the world of technology. Our biggest problem with security at this point, is that we can allow access for faculty and students to various database information, but we do not have sufficient record-level security to control access to a specific record without allowing access to all records.

Many computer administrators have reputations of being dictators when it comes to controlling access to the information for which they are responsible. A good technology manager must find the best balance between access and security. You can't let security control the accessibility of information to the extent that we stifle constructive creativity. Obviously, everyone is going to have a different interpretation of what is constructive and what is not. The other balance that must be maintained is between the right-to-know and the right-to-privacy. We will talk about privacy later, but the core issue here is the unclear view on ownership of data.

I feel that there are two main areas in colleges and universities where improvement in security can have the most effect. The first of these is to make sure that internal security is equally as impenetrable as external security. Too many times, it has been assumed that the only hits on your system are going to come from the outside. Usually most breaches of security come form current staff or an inside person has aided an outside person in obtaining access.

The second area of security that I think is the most important is physical security. This is unlocked doors to offices and computer printouts sitting on desks. Most people do not even think about locking up printouts containing confidential information when they are not at their desk. Many administrators would be surprised to find out how many times information is released to people without any technical security breach. For this reason, sensitive information should probably not be printed on hardcopy unless the person utilizing the printout is willing to accept the responsibility to physically protect the information from being seen by unauthorized individuals.

Since we are charged with the responsibility of protecting any information on our systems, we can't simply accept security breaches as a necessary by-product of IT progress. We must continue to strive to keep or staffs one step ahead of our users and allow them the time and resources to capably monitor and protect our access and files.

Privacy

The "information privacy" issue is probably the most visible and the most important aspect of technology use. Keeping information secure is also the hardest part for users to understand. This is primarily due, I feel, because parts of our lives were previously untouched by technology, so there was no need for concern. Now that technology is part of every aspect of our lives, it is most important that we realize our dependence on technology, and adjust our focus to insure that it is utilized safely and securely.

On the college campus, privacy is just as important as in financial institutions. Grades and financial information are obvious targets for intrusion in our local systems. As a result, the most important regulator of this privacy is the Family Educational Rights and Privacy Act (FERPA). More common names are the Buckley Amendment or just the Privacy Act. Basically this law was provided by the federal government to:

- allow students to inspect and review their educational records
- allow them to have the records corrected or amended
- control disclosure of the content of academic records
- establish requirements about what can and can't be made public
- assure that information is being used for the purpose intended
- require the institution to inform students where data is stored, what policies are being followed, who has the right to see their records, and parental access to records
- specify that those responsible for data systems will take reasonable precautions to prevent the misuse of the data and dispose of information properly and appropriately
- determine when written consent will be required to release any sensitive information and to ascertain what data will be considered private

The key factors here are that institutions should create policies to inform students clearly what their rights are under the FERPA law, assure them that these rights will be maintained, and that the institution will strive to comply with all provisions of the Privacy Act. Obviously how well we secure our systems has a direct relationship with how well we comply with this Act.

Policies

Too many times policies about proper use of technology are simply a list of the "Don't Dos".

This is a negative approach and could possibly provide just the incentive needed by a potential hacker to start hitting on your system. I believe the components of a good policy should:

- clearly differentiate between right and wrong
- be consistent across campus and allow for few deviations or exceptions to the stated rules
- allow for distribution of keys to access areas only when absolutely necessary
- establish acceptable use and tie that usage to the overall mission and objectives of the institution
- clearly state institutional position about possession, copying, and accessing of copyrighted, threatening, violent, trade secret, or obscene data, voice, and video
- state the college rules about personal and commercial use of our resources including: political statements, advertising, game playing, unauthorized e-mail use, pornography, inappropriate language and communications, and any activity utilizing our systems that will reflect negatively upon the college
- define penalties and punishments and clearly describe all private and legal actions that will be taken
- clearly differentiate between unauthorized and authorized access of data, accounts, and files
- define misuse but also develop the policy with direction, philosophy, and guidance as the major thrust of the content
- establish specific rules that apply to using the Internet, World Wide Web, and electronic mail.

It is extremely important to involve representatives from all user communities in the development of "proper use" policies. This brings awareness of what problems are being experienced and a clearer understanding by all of how the policies should deal with various infractions. I also think it is very important to create standard forms on security and use that are completed by faculty, staff, and students upon employment or registration with the college that states basic responsibilities and an assurance that they have read and agree to comply with the overall "proper use" policy.

With this onslaught of inappropriate technology use and illegal activity involving computers, there is a major question of general responsibility for morals and values within our technical world. Who should be responsible for these breakdowns in honest behavior? Among the blamed entities are employers, colleges, high schools, and parents. None of these are exactly jumping up and down and accepting responsibility. Obviously our society and culture are major factors in this puzzle, but neither of these are changed that easily. So what can be done?

Recommendations

There are quite a few unanswered questions, and quite possibly you now have more questions than you had before. There are, however, simple and inexpensive things that you can do to try to improve your protection schemes of critical information on your systems. I recommend:

- teaching IT professionals an appreciation for the social and ethical implications of IT and placing value on private, secure information
- developing an ethics component in technology courses
- insisting on passwords for users that are harder to guess and changing them often
- limit access to required files and functions, only allowing users to see what they can use in the more sensitive areas
- managing users and staff more effectively and knowing what the capabilities are of each individual...awareness is the greatest deterrent to problems
- precise policies that stress acceptable use and not just the things users are not supposed to do
- integrate productive uses of the Internet into the normal workflow and establish rules on usage
- keep up-to-date with current security and privacy breaches and investigate affects on your college
- do not allow any access without investigating the security procedures that must be utilized
- make security policies and procedures for recovery after an incident to be made a part of normal disaster recovery planning
- do not create policies without corresponding enforcement penalties and procedures
- demonstrate and be a role model in ethical and professional use of information technology.

It is clear that we will continue to see advances in both technology and abuse of technology. All we can do is commit more resources for security development, view compliance with the Privacy Act as a minimum, encourage ethical behavior with all user communities and keep aware of what is happening in the technology world around you.

References

Guidelines for Postsecondary Institutions for Implementation of the Family Educational Rights and Privacy Act of 1974 as Amended, American Association of Collegiate Registrars and Admissions Officers, Revised Edition 1995

Forester, Tom and Morrison, Perry (1990). Computer Ethics, MIT Press, Cambridge, Massachusetts.

Rezmierski, Virginia (Fall 1992). "Managing Information Technology Issues of Ethics and Values: Awareness, Ownership, and Values Clarification", Cause/Effect, Vol 15 No 3.

Violino, Bob (1996). "Internet Insecurity: Your Worst Nightmare", Information Week, Feb. 19, 1996.