Global Information Assurance Certification Paper

Topic: Security Policy for Higher Educational Institutions
Author: Steven M. Helwig

Being involved in higher education has made me realized that security is a much needed commodity, but adhering to the "open" academic environment is a requirement. This brief will try to focus on what may be accepted by the academic community while protecting the institution and it's directors. Whether these institutions are federal, state, or private, I believe they will face the same security issues. This is why when searching on the Internet for security policies; most of the findings are from educational institutions. Most attendees at seminars or training again are associated with higher education. I have found this to be an important issue within these institutions therefore I will use knowledge taken from formal training, job experience and other research performed on this topic.

First we must define what the "open" academic environment is. This concept will be the largest issue faced when trying to implement security practices within the higher education domain. It can be conceived by its name that there will be no barriers on information neither coming into nor going from the institution. Is this a practical request? To a security person, invoked to protect an institution's information the answer is probably no. To a faculty member, where educational freedom is a requirement the answer would probably be yes. There are two sides to higher education, the academic side and the administration side. This brings up the question of having two different security models and incorporating them into one policy.

Before a policy can be developed, several assessments must be performed. Current policies must be examined. These must be looked at from both the academic and administration points of view. Meetings can be conducted to get each sides requirements. The network infrastructure must be assessed to verify it is able to meet the requirements. The network infrastructure is critical when designing a security policy. It must be setup so that the academic domain cannot access the administration domain. Thus the network must contain proper sub-netting and security devices installed and configured properly. The type of operating system is also a major consideration when developing these policies. Most higher education environments are heterogeneous and all operating systems security models should be considered.

Besides the assessments listed above, other issues should be produced and or reviewed. A steering committee of concerned parties such as representatives from the student body, academic community and the institute's administration should be formed. Academic Computing, Library Computing, and Administrative Computing should developed computing vision statements to assist in guiding the development of these security policies. Other policies that are closely related with the security policy and may be reviewed or developed at the same time are Internet and E-mail Policies, Incident Handling Policies, Risk Assessment Policy, Data Confidentiality

Considerations, Hardware Failure Recovery, Ethics, and possibly Media Protection Policies and Procedures.

What should the security policy actually address? There are several items that this policy should convey. This policy should be able to ensure all parties concerned that their interests will be protected. Besides the requirements listed below, other service levels should be included in the policy. These are:

- Security controls should be documented and maintained. Should periodically be reviewed and audited.
- Should define the access between authorized users and the networking environment.
- The chain of command responsible for authorization levels. Duties and authorization levels of these positions should be well defined.
- Security Officer or security responsibility duties should be given to some one other than the network administrator or his/her backup.
- This policy should address data ownership, confidentiality, availability, and integrity.
- Data transmission accuracy requirements should be met.
- Data integrity and recoverability requirements should be met.
- A process for detection and reporting of errors should be initiated.
- Most of all, this entire security process should have the approval of the institution's administration and board of trustees. For these policies and procedures to succeed those in any level of authority must understand the importance of and consequences of not having a detailed security policy and procedures.

Below I have listed several typical security requirements that may be required from the administration and academic domains:

Administration Domain

- Restricted access to financial data
- Restricted access to student / admissions data
- Restricted access to alumni data
- Restricted access to marketing data
- Electronic mail (E-mail)
- Access to all campuses
- Access to state or federal agencies (where applicable)
- Access to the Internet

Academic Domain

- Access to the Internet
- Electronic mail (E-mail)
- Access to instructional programs
- Access to state or federal agencies (where applicable)

- Access to all campuses
- Remote access (students and faculty)

Several requirements such as Internet access and E-mail are common but may require different security setup requirements.

Now that we have the security requirements and have looked at the infrastructure, lets look at different areas we need to secure. These should have a presence in your policy:

Physical Security

- Are the servers and networking equipment in a secure area?
- Are the wiring closets secured?
- Are desktops secured? Will a hardware or software lock down device be required for desktops?
- Will access to certain drives be restricted? (What will the security policy be for desktops?)

Login Name Standards

- What will be the minimum length of login names?
- How long will the account be active?
- Will generic names be allowed?

Password Standards

- What will be the maximum time before a password change is required?
- What is the minimum length a password will be?
- Will a password history be initiated and if so how many passwords back will be remembered?
- Are the procedures in place for resetting passwords?
- How many login tries will be allowed before the account is disabled?

Virus Protection

- Is there virus protection on the servers and workstations?
- Are all software programs protected (i.e. E-mail, Internet downloads)?
- Are there procedures in place to ensure that all virus protection is kept updated?
- Is there a policy or procedure if a virus is found?

Auditing

- How will the security policies and procedures be audited?
- Who will perform the audit?
- Who will review the audits?
- What will be audited?
- Is the network, Internet, etc. being monitored? If so, are there policies and procedures in place for this function?
- Are users aware of the consequence of security policy violations?
- Are there proper procedures for the user on reporting security issues or violations?
- Is there a Network Security Officer or someone that is in charge of the Institution's network security?

- Does the Security Officer have the support of the school administration and board of directors?
- Who is tracking patches and security fixes for operating system and application software?

Disaster Recovery / Contingency Planning

- Are there policies and procedures in place for disaster recovery?
- What are the backup procedures?
- Are the procedures tested?
- What are the contingency plans?
- Are periodic "fire" drills performed to test the contingency plans?
- What is the chain of command?
- Is the network plan consistent will other areas of the Institution?
- Is the network plan included in the Institution's master plan?

Training

- Are there policies or procedures for training of facility, students, staff, and others on the Institution's security policies and procedures?
- Are users aware what the security polices and procedures are?
- How are users informed on policy or procedure changes and updates?
- Are there sign off polices or procedures by the users that they understand the policies and procedures and the consequences of any violations?
- Will these consequences or violations be enforced?
- Are all campuses on the same page?

The above areas are topics that are recommended for any security policy or procedure. I have listed them as questions to initiate a thinking process. These topics and questions are by far all that should be considered. If these questions can be answered, then you will be well on your way to a good rounded policy or procedure. In the proceeding sections, recommendations and other considerations will be discussed.

The recommendations that are listed below are just that, recommendations. These are a compilation from several Universities, business experience, and from books on security management.

Physical Security

- Have a UPS (Uninterruptible Power Supply).
- Workstations should have power protection.
- Servers should be in limited access locked rooms.
- Post warning signs about cables and pulling electrical plugs.
- Ensure that there is adequate backup power.
- Wiring closets should be kept locked.
- Users should utilize anchoring devices along with hardware and/or software security devices on their workstations.
- Maintain maintenance agreements.
- Warn users never to leave laptops unattended.

- Ensure that cabling, plugs and other wires are protected from foot traffic.
- Develop and maintain an asset control system that will keep records of all computing and networking equipment and software.
- Check network configurations regularly.
- Maintain logs of all network transactions and review daily.
- Ensure that security related events are immediately posted and acted on in a timely matter.
- Record and report all network malfunctions. Document corrective actions.

Login Name Standards / Logins

- Every user accessing the network should have a unique User ID and only one ID.
- Do not use Guest login accounts.
- Ensure user accounts do not default to a Guest account.
- If a Guest account must be used, password protect it.
- Allow Grace login periods not longer than 5 days.
- Allow only a maximum of 5 unsuccessful login attempts.
- Access to computer systems should be suspended after the user has logged out.
- Should not allow any group accounts unless there is written authorization from a person empowered to authorize these types of requests.

Password Standards

- All accounts must have a password.
- Passwords must not be shared.
- Passwords should be encrypted and not transmitted in clear text format.
- Passwords should be a minimum of 6 alpha and numeric characters.
- The user and the network operating system should only know the password.
- Passwords should be checked against a password-checking program.
- Password history should not be allowed.
- Password expiration should be 30 – 90 days in length. For students it could be per quarter (accounts can be disabled and if student re-registers the account is enabled and password change should be forced).
- If the user forgets their password, a temporary password is given and the account is forced to change the password on first login.

Virus Protection

- Servers should have a virus scanning and cleaning program installed.
- Virus programs should be updated regularly if not automatically.
- The use of diskless workstations may be considered.
- User computers and workstations should also contain a virus program

and this program also should be updated regularly if not automatically. This program should also be able to check not only the hard drives but also floppies and removable drives.

- Document procedures of cleaning and scanning process and ensure the users are trained to perform these functions.

Auditing

- All unauthorized copies of software should be removed from computers.
- Review audit logs on a regular basis.
- Any breach to systems or the network should be investigated.
- Intruder alert facilities should be activated and all alerts should be acted on.
- Audit department or a third party auditing firm should perform periodic network audits. The results should be reviewed and acted upon.
- Auditing software should be run periodically and compared to security policies and procedures for discrepancies. These should be corrected immediately.
- Audit procedures should be generalized and also contain specific audits by operating systems (i.e. NT, UNIX, Mainframes, Novell, Linux, etc.).

Disaster Recovery / Contingency Planning

- Backups should be automated and be performed nightly. At a minimum, a weekly incremental and a full monthly backup should be considered.
- Backups should be tested to ensure that when needed, recovery could be performed.
- Users should be trained to store important files on the servers so these files will be backed up when the system backups are performed.
- Several generations of backups should be maintained with the latest copy kept on site and the others off-site. A good tape (media) rotation plan is important.
- Maintain complete and accurate backup logs and ensure media is properly labeled. Good backup procedures are essentials.
- Contingency and Recovery plan should be tested and revised as needed.

Training

- Users should be made aware of security policies and procedures. Especially of the consequences to violations of these policies.
- Network administrators and their backups should be properly trained.
- Periodic training of users on updates should be performed.
- Ensure network administrators know what logs to gather information from and how to read and analyze them.

Along with the above standard topics that should be included in your security policy, lets look at some other considerations.

Other Considerations

- Remote Access
  - Require callback mechanism.
  - Ensure logging is initiated.
  - Access to network must be able to authenticate the user.
  - Persons requiring remote access should have written authorization.
- Software Security
  - Develop a software management program. All software should be maintained by the IT department and secured.
  - The IT department should only acquire software. Software development policies and procedures should also be co-developed by the IT department.
  - All software should be tested before being put into production systems. This includes purchased and developed software products.
- Network Security Responsibilities
  - Protect network from outside entities.
  - Protect transmissions sent over the Internet.
  - Transmit information securely.
  - Backup information.
  - Store information properly.
  - Dispose of information in a timely and thorough manner.
  - Present information for use in a secure and protected way.
  - Protect the network from unauthorized access.
  - Limit or prohibit unauthorized sharing of users rights.

The intent of this document is to assist institutions of higher education to begin to develop a detailed security policy. I would like those that read this document to come away with ideas and thoughts on how they can develop their security document. These recommendations are not set in stone but are typical in a higher education environment. It is important to get as many ideas or requirement from all departments within your institution. Every department should have some say in its development. This will also make it easier to enforce. I also want to emphasize the importance of Administration and or board by in, so these policies and procedures may be properly enforced. I would also recommend review other institution's documents, most of which can be reviewed on the Internet.

Bibliography

Internet Sources
Brown University "A Survey of Selected Computer Policies from Institutions of Higher Education" 1996 URL: http://www.brown.edu/Research/Unix_Admin/CUISP

Columbia University "LAN Security Guidelines"
URL: http://www.ais.columbia.edu/ais/html/Lan_security_guidelines.html

Computer and Academic Freedom Project Academic Freedom Information 1999
URL: http://www.eff.org/CAF/

Cornell University "Policy Digest" Updated 5/23/2000
URL: http://www.cit.cornell.edu/computer/policies/digest.html

MIT Information Systems "Infrastructure Requirements for Applications and Systems"
August 4, 1998 URL:
http://web.mit.edu/is/integration/doc/requirements.html#netsecurity

National Center for Education Statistics "Safeguarding Your Technology" 11/18/1998
URL: http://nces.ed.gov/Pubs98/Safetech/

Penn State University Computer Network and Information Security 4/22/1997
URL: http://www.guru.psu.edu/policies

University of New Mexico Security Updated 12/08/2000
URL: http://www.unm.edu/cirt/security/#checklist

University of North Texas "UNT Information Resources Security Policy" 8/91
URL: http://www.unt.edu/planning/UNT_Policy/Volume2/3_6.html

University of Toronto Computer Security Administration Updated 12/13/2000
URL: www.utoronto.ca/security/LAN.html#LAN

Books
Krause, M. and Tipton, Harold F. (Eds.), Information Security Management Handbook 4th Edition, Boston: Auerbach, 1999.

Krause, M. and Tipton, Harold F. (Eds.), Information Security Management Handbook 4th Edition Volume II, Boston: Auerbach, 2000.

Bosworth, Seymour, and Hoyt, Douglas B. and Hutt, Arthur E, (Eds.), Computer

Security Handbook 3rd Edition, John Wiley and Sons, 9/1995.