Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Security In An Open Environment Such As A University?

With myriad aspects to address in establishing cyber security, an easy concept to overlook is the relationship between information security and the attitudes and perspectives that influence the process of developing an information security strategy, especially in an open network environment like a university. This paper will discuss a definition, the needs, and the goals of an open environment like a university; examine a process of developing an authorized framework and team for university information security; presen...

Copyright SANS Institute
Author Retains Full Rights

AD

Table of Contents 1
Carol_Templeton_GSEC.doc 2

© SANS Institute 2005, Author retains full rights.

SECURITY IN AN OPEN ENVIRONMENT SUCH AS A UNIVERSITY?

Carol Templeton
December 21, 2004
GSEC Practical v 1.4c, Option 1

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

ABSTRACT

With myriad aspects to address in establishing cyber security, an easy concept to overlook is the relationship between information security and the attitudes and perspectives that influence the process of developing an information security strategy, especially in an open network environment like a university. This paper will discuss a definition, the needs, and the goals of an open environment like a university; examine a process of developing an authorized framework and team for university information security; present some of the attitudes and perspectives that can help or hinder security implementation, as revealed through personal experience; and identify security resources that can be used for effective information security development and improved security perspectives.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

CONTENT

Abstract 2

Defining the Environment, Needs, and Goals 4
- Definition 4
- Needs 4
- Primary goal 4

Development of an Authorized Security Framework and Team 5
- Watch Dog without Authority 5
- Leadership by Example 6
- First Line of Offense 6

Recognizing Perspectives, Attitudes, and Their Effects 7
- Management Perspectives 7
- Clash of the Technicians 7
- Easy for Staff 8
- Faculty Concerns 8
- Student Attitudes 9
- OS Bias 9

Information Security Resources Affect Perspectives 10
- Education for Management 10
- Common Ground for Technicians 13
- Elevating Awareness for Faculty, Staff, and Students 14

Conclusion 18

References 19

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

DEFINING THE ENVIRONMENT, NEEDS, AND GOALS

Implementation of information security in an open environment like a university must begin by defining the environment; followed by determining the needs and goals within the environment. These are major steps in the development process of an information security strategy.

The **definition** of a university environment is a complex construct that defies cookie cutter choices for information security solutions.

- A university environment is inherently open by nature; providing equal availability of knowledge; without restriction of freedom of thought or information.
- Universities are public and private and operate within a multiplicity of government regulations. Private universities are generally more autonomous and freer to define and implement security policies and procedures.
- Ownership of a university infrastructure is also more complex. Departments within universities claim levels of autonomy based on the belief that they are responsible for the funding of their department and should be the sole authority in determining the level of security within their department.
- Unlike corporations, a university acts within the scope of the information provided by defined goals. "Rule by edict" is not realistic in a university environment.
- Universities are continually competing for students, research grants, alumni gifts, local, state, and federal funding; granting scholarships; selling books, supplies, housing, nourishment, etc.; thereby establishing financial responsibilities.

The **needs** of a university environment are direct extensions of the definition of the environment.

- To provide "…an atmosphere that encourages free exchange of ideas, and an unwavering commitment to academic freedom." [1]
- To provide a network infrastructure capable of supporting diverse network demands and expectations.
- To protect the infrastructure from unwanted activity and/or restrictions; both internally and externally.
- To provide cohesive, comprehensive security policies and procedures that will not become "shelfware" [2]; required to have but not used because they're too confusing to follow.
- To strive to adhere, insofar as resources will allow, to all legislative requirements

© SANS Institute 2005 Author retains full rights.

The **primary goal** of a university environment is education; with related goals of:

- establishing and protecting a positive reputation
- funding
- community enrichment

[1] The University of Tennessee, AUP, p. 1
[2] Desilets, p. 1

Universities often find these goals at odds with the establishment of adequate security policies and procedures. Questions are continually presented against information security processes such as:

> "Who are you to tell me what to do with my computer?"
> "Why are there so many rules to follow?"
> "Why does this cost so much?"
> "Why is more staff required?"

The attitudes and perspectives adherent to this diversity of issues makes security policy and procedure a nightmare-come-true for a security administrator and staff. With the environment, needs, and goals defined for a university, the next concept is developing an information security strategy.

DEVELOPMENT OF AN AUTHORIZED SECURITY FRAMEWORK AND TEAM

Security planning requires approval and comprehension from the top at the very beginning. Trying to implement security from a grass-roots level can often be haphazard and perspectives regarding security can make or break a security plan very quickly.

Watch Dog without Authority

The first attempt at network security for the university, where I am employed, consisted of a single person acting as a watch dog for the network. Like a watch dog, that person attacked security incidents as they occurred. The problem with this approach was the unbridled remediation efforts employed, often with large amounts of personal bias applied. This kind of watch dog attitude might work well in a very small personal network environment, say a single computer, but it definitely doesn't work at a university. The attitudes and actions exhibited severely offended several levels of upper authority and the person was removed from the position.

The next attempt at network information security by the university's security group, of which I am a member, was more successful. Representatives from several departments on campus, mostly technical, comprised a committee to write information security policies and procedures; but the authority for the plan implementation was not established. While technical expertise is certainly a vital part of the information security process, the authority for implementation is an imperative.

© SANS Institute 2005 Author retains full rights.

After 18 months of developing what was thought to be valid, useful policies and procedures, the documentation was presented to upper management for approval and promptly vetoed based on the lack of prior documented authority for implementation of the plan. It wasn't enough to have documents that told people how to secure their systems and network; there had to be a framework establishing a valid authority to develop and enforce the information security initiative and it needed to come from the top.

Leadership by Example

After September 11, 2001, President George W. Bush exhibited his authority, approval, and involvement in cyber security by defining a framework that would protect the Nation from cyber-terrorism. In the Executive Summary of the "National Strategy to Secure Cyberspace", the President invited "the creation of, and participation in, public-private partnerships to raise Cybersecurity awareness, train personnel, stimulate market forces, improve technology, identify and remediate vulnerabilities, exchange information, and plan recovery operations." [3]. In the Actions and Recommendations Summary of the same document, (A/R 3-5) the definition of the expected role of colleges and universities was documented. "Colleges and universities are encouraged to secure their cyber systems by establishing some or all of the following as appropriate: (1) one or more ISACs to deal with cyber attacks and vulnerabilities; (2) model guidelines empowering Chief Information Officers (CIOs) to address Cybersecurity; (3) one or more sets of best practices for IT security; and (4) model user awareness programs and materials." [4].

David Ward, President of the American Council on Education explained the need for authoritative support from upper management in his article "Letter to Presidents Regarding Cybersecurity" published in Eye on Washington. The article states, "As with any major institutional initiative, success depends on education, resources, people, management, policies, and, above all, leadership. As the President of your institution, you have an essential role to play in the effective deployment of computer and network security on your campus." [5]. It is imperative to develop an initiative that is blessed by the highest level of authority at a university to set the tone for acceptance of security by the entire campus. Top-level involvement and approval establishes and supports defined paths of authority for implementing, documenting, and enforcing security policies and procedures.

First Line of Offense

With an approved information security initiative established, assembling an authorized security team is the next step. This security team will be ultimately responsible for the development of information security policies and procedures that will affect the entire university and they should possess strong technical and social skills. They must be able to collaborate with network and system administrators on the technical issues and needs of the infrastructure; advise and seek advice from all levels of management and their associated administrative staff; and educate the campus community in recognizing what their roles and responsibilities are in information security. This step is particularly important because this phase of information security planning will either be a successful gathering of allies or a collection of determined adversaries. It is

© SANS Institute 2005 Author retains full rights.

during this stage of plan development that attitudes and perspectives become most visible and active.

[3] National Security Strategy to Secure Cyberspace, p. xiii
[4] National Security Strategy to Secure Cyberspace, p. 58
[5] David Ward, "Letter to Presidents Regarding Cybersecurity"

RECOGNIZING PERSPECTIVES, ATTITUDES, AND THEIR EFFECTS

If information security was dependent on a single issue, goal, or person it would be very simple to implement. Instead information security is a complex concept and requires complex responses. To effectively secure any network infrastructure, the task must be directed from the notion of "Defense in Depth". [6] This perspective and must be applied to the acquisition of personnel as well as equipment. There is no "silver bullet" to prevent or resolve all security incidents and there certainly is no "magic potion" to ensure the complete agreement or cooperation of all persons involved in the development of an information security plan. In the efforts to implement information security at the university, where I work, we encountered issues and perspectives that are common to most universities.

Management Perspectives

Upper management must be the final voice to balance all facets of information security with university needs and goals. With a reputation to consider at all times; negative responses to security incidents directly impact enrollment, grants, research funding, the relationship between the university and the surrounding community, and the attraction of world-class faculty and staff. Upper management must be aware of all the ramifications of an insecure information infrastructure.

For management, budgeting is a real concern and the most common perspective, especially at educational institutions where funding is a scare commodity, is to implement the most security possible with the least amount of expense. While this is not an unusual perspective, given the budget constraints of today's economy, it is one that makes the implementation of an information security strategy difficult. While it may often appear to management that much of their budget is being spent on seemingly superfluous equipment or personnel: it is because they don't always see the return on their investment as tangible. Management should rely on a business impact analysis for assistance in determining the costs associated with risks and on the input of information security staff for the best methods of remediation in terms of equipment and personnel.

Clash of the Technicians

Attitudes and opinions among technicians are as varied as the types of network equipment and operating systems available today. At the university where I am employed, network design spawns most of the differences of opinion between network and security technicians. Network engineers are concerned with the nuts and bolts of

© SANS Institute 2005 Author retains full rights.

building and maintaining the network and equipment. Usually, their focus is with bandwidth, traffic shaping, speed of communication, network connectivity (wired or wireless), and the continued ability to connect to the world via the Internet; in other words, the availability of the network. They adopt a very strong sense of ownership of the network and are not willing to have anyone interfere or tell them how to build or maintain the network.

[6] Eric Cole, p. 18

Information security technicians are equally focused on availability, but their efforts are also aimed at the confidentiality and integrity of the network by preventing system compromises and malware. Information security personnel perform vulnerability assessments and, as a result, often find vulnerabilities in an infrastructure that may be obscured from a network engineer's perspective.

By focusing on a balance of the principles of confidentiality, integrity, and availability [7] network engineers and security technicians can design a highly functional, reliable information infrastructure that includes security from the design phase through the maintenance phase; and is reiterated throughout.

Easy for Staff

Network authentication and accessibility directly impact university staffs; who are concerned with how information security will affect their daily routines. The main issues will be "Why do I have to comply?" and "Will it be easy to do?" Intrinsically, people do not want to be watched, tracked, monitored, or ordered about. The need for information security policy and procedure *can* initially offend one's sense of integrity and privacy. It will not instinctively occur to some people that information security could be more beneficial to them than intrusive.

Daily use manifests a strong sense of ownership of a computer. Once the computer is configured just the way one wants it, one is reluctant to allow anyone changing anything on one's computer or being *instructed* to change anything. Personal attachments are evident in the pictures of family, pets, hobbies, or beliefs used as wallpaper on their systems. When problems arise with the computer, perspective takes a dramatic shift. Ownership of the computer and its contents is retained, but the ownership of the problem and responsibility for remediation is sometimes relinquished.

Faculty Concerns

Faculty is concerned that security will be a means to restrict the ability to freely impart knowledge. Since some security policies and procedures will deal with what is, and what is not, allowed to be transmitted across the university network, this is sometimes viewed as an infringement upon a constitutional right to free speech or the inhibition of academic freedom.

Just as with technicians and staff, a strong sense of ownership develops but is directed toward the subjects taught, the materials used, the methods and means of

© SANS Institute 2005 Author retains full rights.

disseminating class material, and communicating with students and peers. Classes are increasingly taught via web broadcasts to accommodate the increasing number of students. Homework and grades are assigned and posted on web sites. Network down time and system access difficulties are not tolerated since they interfere with faculty's primary goal of teaching.

[7] SANS GSEC Security Essentials training materials, Book 1-2, p. 15

Student Attitudes

Student perspectives regarding information security evolve from a sense of youth, and all that implies, more than any other single factor. These are young adults generally encountering their first taste of freedom and they actively resist any form of restriction or regulation.

Where once a quality pen and pencil set was considered an appropriate gift to a young graduate; today, computers are a necessity. Because students own their computers, the perspective is that they can do as they like with their own property. As a result of paying fees for network access, the network is viewed as a service, bought and paid for, and the attitude of doing as one pleases is extended to the use of the university infrastructure. The average student is either unaware of the responsibility to comply with established security policies, or they don't care.

Of particular interest, at the university where I work, was one student's attitude regarding copyright infringement. The opinion expressed was that the music industry charged too much for DVDs, CDs, and tapes. Despite the willful knowledge of committing a crime, this person was pirating software and music in protest of the pricing. Another common perspective expressed is "Everyone else is doing it." Peer pressure, ignorance, and defiance are difficult for security staff to combat.

OS Bias

Another perspective that permeates all categories of users is operating system bias. There is a mixture of Windows, Linux, UNIX, and Apple users at the university where I am employed and each category of these users are very vocal in the defense of and the belief in the impregnability of particular operating systems. This false belief is strong despite:

- the recent emergence of a root-kit designed to specifically target Mac OS X systems [8]
- a fake security alert email circulating in the wild that is aimed at Fedora-RedHat Linux systems [9]
- the published findings of a recent mi2g Intelligence Unit study analysis that determined "…Linux has become the most breached 24/7 online computing environment in terms of manual hacker attacks overall and accounts for 65.64% of all breaches recorded, with 154,846 successfully compromised Linux 24/7 online computers of all flavours."; and that "…Windows has become the most

© SANS Institute 2005 Author retains full rights.

breached computing environment in the world accounting for most of the productivity losses associated with malware - virus, worm and trojan - proliferation." [10]

[8] MacInTouch Reader, 22 October 2004
[9] K-OTik – Fedorah-Redhat Fake Security Alert, 28 October 2004
[10] mi2g , News Alert, 2 November 2004

There is also a tendency to forget about the various threats to the software applications installed on systems and to gloss over the published announcements regarding vulnerabilities.

INFORMATION SECURITY RESOURCES AFFECT PERSPECTIVES

Once the definition and needs of the university environment are established, top-level approval and support are obtained, a security team is established, and the existing perspectives regarding information security are identified; the next step is to identify the information security resources and methods best suited to meet the needs of the university environment. The security resource of most value is education.

Education for Management

The education of management should include answers for why information security is an imperative, recommendations for budgeting and funding resources, information regarding applicable legislation, and technical communication skills.

One of the most damaging security vulnerabilities experienced by IT management, at the university where I am employed, was the near-crippling infection by the Blaster and Welchia worms at the beginning of the Fall Semester of 2003. When advised to immediately isolate known infected systems at the onset of the incident, management opted to not shut down any of the systems for fear of the loss of credibility within the campus community. Remediation of this incident required an enormous amount of time and man-power to stop the spread of infection and to clean the infected systems. The price of this disaster clearly revealed the need for security awareness training, at all levels, to affect a change in perspectives regarding information security. Management needs to maintain a broader perspective regarding information security issues, but they also need to be sure their perceptions are accurate. There are classes offered by the SANS Institute [11] that are tailored for management education.

- Security 309: Intro to Information Security (Track 9) – offers a fast way for managers to "Master risk management, security management, access controls, attacks and counter measures, secrecy and privacy, along with auditing concepts." [12]
- Management 414: SANS®+S™ Training Program for the CISSP® Certification Exam (Track 14) – offers an understanding of the "critical areas of network

© SANS Institute 2005 Author retains full rights.

security" and "Each domain…is dissected into its critical component. Every component is discussed showing its relationship to each other and other areas of network security." [13]

[11] SANS Institute - (SysAdmin, Audit, Network, Security), p. 1
[12] SANS CDI East 2004 ~ Intro to Information Security, p. 1
[13] SANS CDI East 2004 ~ SANS® +S™ Training Program for the CISSP® Certification Exam, p. 1-2

- Management 512: SANS Security Leadership essentials for Managers (Track 12) – offers "… vital, up-to-date knowledge and skills required to supervise the security component of any information technology project." And "… is designed to empower senior and advancing managers who want to get up to speed fast on information security issues and terminology." [14]

Knowledge of the costs associated with information security is necessary for management and technicians. Loose or non-existent security is always costly in terms of man-power, reputation, possible litigation, and the loss of other intangibles. Prevention can cost less than recovery from crippling incidents. Technical engineers can balance the physical requirements of the university network with available information security technologies and equipment that will best suit the current network infrastructure. Engineers must be prepared to offer cost effective solutions to management that address the mitigation of threats.

Larger universities may find it easier to allocate funds for a security program as part of an existing maintenance schedule for the network infrastructure. Smaller universities may encounter significant difficulties in affording the equipment and personnel to support any effective information security program because of lack of funding.

No matter what size the university is, management must be aware of all the options available for obtaining funding to augment the security budget. Most recently, The Homeland Security Advanced Research Projects Agency (HSARPA) [15] listed several active solicitations for research and development funding available to universities. Of particular interest is Broad Agency Announcement 04-17 [16], an offer of government funding in the research of tools and methodology for:

- creation of more secure systems
- vulnerability prevention, discovery, and remediation
- security assessment
- critical infrastructure protection
- wireless security
- network attack forensics
- defense against identity theft

Knowledge of the current laws governing a university will empower management and

© SANS Institute 2005 Author retains full rights.

technicians when developing an information security program. It is advisable for a university with multiple campuses to have a single set of overall information security framework requirements while also allowing for the creation of tailored, detailed policies pertinent to the needs of satellite campuses.

---

[14] SANS CDI East 2004 ~ SANS Security Leadership Essentials for Managers, p. 1
[15] HSARPA, Solicitations and Teaming Portal, Oct. 19, 2004
[16] BAA 04-17, Cyber Security Research and Development (CSRD), Proposer Information Pamphlet, Sept. 9, 2004

Understanding the diverse curriculums and services offered at satellite campuses will provide a good basis for applying remediation to meet the needs of applicable regulations and for establishing the requirements for compliance to these regulations.

The current primary federal laws governing universities are:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) – for institutions that provide health care or are affiliated with health care providers [17]
- Family Educational Rights and Privacy Act (FERPA) – protects the privacy of student education records [18]
- Gramm-Leach-Bliley Act (GLBA) – requires the security and confidentiality of personal information, such as names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, and Social Security numbers, gathered by financial institutions. [19]

Universities that offer an agricultural curriculum may find that they also fall under the jurisdiction of The Public Health Security and Bioterrorism Preparedness and Response Act of 2002. This act addresses national, state, and local preparedness and response planning, reauthorizes or amends established grant programs, and establishes significant new grant opportunities for state and local governments [20].

Financial activity is an important area where universities must employ responsible information security strategies. In an interview with Jack McCarthy, leader of PricewaterhouseCooper's National Education and Nonprofit practice, McCarthy stated that "Higher education institutions don't take their fiduciary responsibilities lightly…and their audit committee members take their duties as seriously as if they were sitting on the board of Ford or GM. When you think about it, colleges are actually in the education business, the housing business, the entertainment business, and the research and health care businesses, among many others. Even without the same rigorous auditor-rotation or certification issues as public concerns, there are many practical changes they should be making." [21]. McCarthy's comparison of universities to businesses supports the definition of a university environment as a business entity and supports the need for an information security plan that can protect a university with increased fiduciary accountability. In the same interview, John Mattie, leader of PwC's Education Advisory Services practice, stated that "Larger university audit committees might have someone from the corporate world who is a financial expert as defined by

© SANS Institute 2005 Author retains full rights.

Sarbanes, but the smaller colleges should be bringing more financially literate members onto their committees."[22].

[17] HIPAA, Sept. 16, 2004
[18] FERPA – 20 U.S.C. §1232g; 34 CFR Part 99
[19] Federal Trade Commission – Facts for Business; Financial Institutions and Customer Data: Complying with the SafeGuards Rule, Mar. 26, 2003
[20] National Conference of State Legislatures, Nov, 23, 2004
[21] Jack McCarthy, PricewaterhouseCoopers ©2002, Business Archive, July 2004
[22] John Mattie, PricewaterhouseCoopers ©2002, Business Archive, July 2004
Matties' recommendation supports the need for development of a security team strong enough to assist management with risk analysis and budgeting as well as having enough knowledge to collaborate with network technicians in developing an information security plan that is adequate to protect a university.

Universities will inevitably host students from geographic areas outside the immediate locality of the institution. While universities are not bound by the laws of other states, management and technicians must include consideration of possible inter-state requirements in the development of an information security plan. For example, New York limits the use of Social Security Numbers in schools and colleges while California bars businesses, health care providers, and schools from publicly posting Social Security Numbers, printing them on cards for accessing services, requiring them for access to web sites unless they are accompanied by a password, or printing them on materials mailed to an individual [23].

While these are just a few of the areas where management needs to be informed, they are a good starting basis. In addition, management should be familiar, and coordinate, with the university legal and audit departments to insure adherence to any and all information security requirements. Cultivating an accurate picture of information security requirements increases management's confidence in information security decision making. Management can become more supportive and understanding of technical staff and the challenges faced in developing information security strategies.

Common Ground for Technicians

As discussed previously, President Bush, in the National Strategy to Secure Cyberspace, mandated the creation of information sharing resources to promote cyber security. When designing a university infrastructure, technicians can tap these security resources to share and learn from the experiences of their peers. By using information resources such as Netigy, EDUCAUSE, SANS, and UNISOG (University Security Operations Group), technicians can focus on two very important concepts in network design:

- avoiding others' mistakes
- working in a cooperative effort to provide information regarding possible or imminent threats

© SANS Institute 2005 Author retains full rights.

Netigy Corporation offers documentation on security architecture through SABSA, the Sherwood Associates Business Security Architecture methodology. [24] In his Executive White Paper for Netigy [25], John Sherwood explained that determining what network architecture should be built can be boiled down to three factors:

* goals * the environment * the technical capabilities

[23] MSN Money, "Safeguard your Social Security Number", August 20, 2003
[24] Netigy, SABSA®, Copyright © 2002
[25] John Sherwood, CISSP, "SABSA ® Security Architecture", p. 1

Sherwood continues to explain that information security architecture, if built correctly, is more like assembling all the parts of a car in the correct order. As each section is assembled, a different layer is added to the whole construct. [26]

EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. [27] EDUCAUSE serves as a central repository of shared information in the areas of cyber security, information systems and services, technology management and leadership, libraries and technology, networking and emerging technologies, policy and law, and teaching and learning. [28]

SANS leads the industry in providing world wide, respected, valuable, training and certification for security professionals at all levels of technical and managerial responsibility. SANS also provides free availability to the largest international collection of information security research documentation.

UNISOG provides several venues of communication for security professionals. The requirement for joining this listserv organization is very straight forward, "Membership is restricted to people who actively work to secure their educational sites network and systems in a suitable fashion as a staff member." [29].

These resources provide cooperative, current, avenues for technicians and management to stay informed of issues that can specifically affect university environments. Sharing experiences and discoveries that work best in a university environment can help technicians reduce mistakes in network design and implementation. With information security built into the network, technicians can provide effective information security plans to management to help with the development of polices that work in tandem with the construction of a secure network. With more cooperative attitudes established, technicians have provided themselves with mechanisms to develop the larger picture they need to see making them more effective team members.

Elevating Awareness for Faculty, Staff, and Students

Faculty, staff, and student attitudes are often the most difficult to address due to the shear volume of these groups at a university. All three of these populations of users

© SANS Institute 2005 Author retains full rights.

view ownership of the network differently and can sometimes be adamant in wanting a voice in the development of governing security policies and procedures. Again, education and awareness are an absolute must for these groups. The level of education for these groups doesn't necessarily need to be as in depth as for management or technicians, but it does need to be relevant to their positions in the university community.

[26] John Sherwood, CISSP, "SABSA ® Security Architecture", p. 5
[27] EDUCAUSE, About EDUCAUSE, Dec. 5, 2004
[28] EDUCAUSE Resources, Dec. 5, 2004
[29] UNISOG Home, Dec. 21, 2004

These groups need to become part of the security solution, rather than exist as issues in a security problem. Making these groups a part of the security development process takes their needs into account in the design process. Participation in this solution offers a communication outlet that is invaluable; the freedom to express ideas that are important to a specific group.

There are several ways to incorporate these groups in decision processes.

- Inviting members of departments to participate in the policy making process.
- Developing remediation processes that are feasible within the technical capabilities of each group.
- Providing information and support for groups that are not technically well informed.
- Making the consequences of actions better understood

While decision making by committee is not easy, it will insure that as many perspectives as possible have been considered with any given information security issue. A technical security committee is essential to the approval process of information security policies and procedures. This committee should be comprised of personnel that are most familiar with the current information infrastructure and university business practices. Sub-groups of committee members can reduce the overall documentation development time.

Once a policy is developed and approved by the technical security committee, the document should go before a review board to be checked for regulatory compliance and with current university business practices. This review board should serve as a final check point before presenting the documentation to upper management for approval. Membership in these committees will provide insight for the need of information security policies and address the questions of information security policies adherence.

Operating system hardening guides are excellent educational tools that provide a practical view of system security to users based on the operating system they have chosen. These guides, based on industry best practices, can be applied manually by users but, at the university where I work, support staff has combined them with the

© SANS Institute 2005 Author retains full rights.

network's initial registration process to create a utility that enables users to easily install patches and anti-virus software. In this manner, improved information security is enforced but made easy because it is automated. Additionally, by providing users an awareness of current information security issues and vulnerabilities and giving them an easy to use tool to remediate security problems, it is possible to support and encourage a sense of ownership and shift attitudes from apathy to necessity.

Faculty's issue with the possible suppression of freedom of expression can be addressed if they are assured of continued communication between faculty, students, and peers. At the university where I am employed, faculty are usually supplied with the computers they use in their teaching; making the equipment the property of the university and not the person.
As such, the university has a responsibility to support that equipment. Management must be diligent in the employment of effective, trained personnel familiar with current information security practices to support the faculty. Faculty attitudes and perspectives can be changed to foster a greater degree of trust if it is proven that what they are teaching is not being restricted; while being made aware that the instructional process is being improved with regards to confidentiality, integrity, and availability.

Copyright infringement is one issue that permeates universities. Peer-to-peer and file sharing software are not, in themselves, illegal to own or use; but some of the activity performed with the software is illegal. This is an area where information security education is also effective. Defiance in the face of knowledge, and peer pressure, can be successfully addressed if the consequences of illegal activity are known and enforced.

The Digital Millennium Copyright Act (DMCA) "…creates two new prohibitions in Title 17 of the U.S. Code—one on circumvention of technological measures used by copyright owners to protect their works and one on tampering with copyright management information—and adds civil remedies and criminal penalties for violating the prohibitions." [30] In more simple terms, the DMCA made it illegal to access copyrighted work without prior authorization of the rightful owners; illegal to make copies of copyrighted work without prior authorization of the rightful owners; and made provisions to govern certain devices and circumstances that could be proven to have been created for the express purpose of circumventing the mandates of the DMCA. [31]

The Recording Industry Association of American (RIAA) has based litigation efforts on the premises established by the DMCA to protect the interests of their clients and have even offered amnesty [32] to offenders if they would cease and desist in their illegal activities.

Universities, serving as ISPs to their campus community, have a legal responsibility to address known acts of copyright infringement and impose penalties for repeated offenses. At the university where I am employed, remediation efforts range from instructional discussions, to letters of reprimand in student or personnel folders, to more stringent penalties such as termination of use of the network.

© SANS Institute 2005 Author retains full rights.

Separate from the illegality of the sharing of copyrighted material are the vulnerabilities introduced on a computer using file sharing software such as KaZaa and Gnutella. Because a user's system must be open to utilize such software; users are, in effect, offering their system to any hacker in need of a conduit for malicious activity. Ignorance is a far more remediable issue by explaining the effects of file sharing. Education is sometimes sufficient to eliminate illegal activity and system vulnerabilities introduced by peer-to-peer programs.

[30] DMCA, 1998, p.2
[31] DMCA, 1998, p.4
[32] Yahoo!News, Australia & NZ, Sept. 5, 2004

Secure passwords, anti-virus software, anti-spyware/adware programs, host based intrusion detection/prevention systems (HIDS/HIPS), host based firewalls, and current critical operating system and application patching are the minimum suite of tools and practices that users should employ to protect their systems. Offering education, knowledgeable support, incentives for security compliance, and free utilities, can create a powerful security resource: a community of users that are more personally involved in learning about, and acknowledging a sense of responsibility for, information security. Even the Federal Trade Commission is considering offering bounties to users that will report spammers to the authorities and assist in bringing them to justice. [33]

Utilizing the media, in as many different forms as possible, is a very powerful security resource. The university where I work has recently approved the establishment of a "Security Month" aimed at increasing the awareness and education of faculty, staff, and students regarding information security. Ads will be placed in local newspapers. Information security classes will be required for Resident Advisors in the dorms to increase awareness of their responsibility in the enforcement of information security policies and procedures. Videos will be aired to present the most common practices of information security that are easily implemented by users. Fliers placed in pay envelopes will remind many that they have a personal responsibility in protecting the university's network infrastructure. The ultimate goal is to use all resources available to "get the word out".

© SANS Institute 2005 Author retains full rights.

[33] Will Sturgeon, silicon.com, Sept. 17, 2004

CONCLUSION

Even though the terms "security" and "open environment" are not synonymous, they can be combined in a working relationship. There are many more aspects of information security than the ones presented here, but the issues discussed in this paper are crucial to the complexities of a university environment. If an information security professional, whether a manager or technician, is not aware of the defining factors, needs, and goals of their environment; critical steps are missed that will weaken the entire framework of the security strategy. If the authority for information security implementation and enforcement is not established at the beginning, the efforts will flounder in a sea of conflict, apathy, and misdirection. If information security management and staff are not technically and socially skilled, they can be the instigation of animosity instead of cooperation. If the entire university community is not involved and educated, they can't, and won't, develop the attitudes, perspectives, and sense of ownership and personal responsibility needed to support the relationship between information security and academic freedom. As an information security professional, it can be challenging and exciting to be a part of this relationship at a university. The openness of a university presents information security professionals with a kaleidoscope of opportunities to meet each challenge with tried and true security resources as well as constant possibilities to develop innovations of their own design. Can there be information security in an open environment such as a university? Absolutely!

© SANS Institute 2005 Author retains full rights.

REFERENCES

1. The University of Tennessee Information Technology Acceptable Use Policy (AUP), 19 May 2004 URL: http://oit.utk.edu/aup (28 Sept 2004)

2. Desilets, Gary. "Shelfware: How to Avoid Writing Security Policy and Documentation That Doesn't Work", 20 Apr 2001 URL: http://www.giac.org/practical/gsec/Fary_Desilets_GSEC.pdf (28 Sept 2004

3. Executive Summary, p. xiii; "The National Strategy to Secure Cyberspace" URL: http://www.whitehouse.gov/pcipb/executive_summary.pdf (29 Sept 2004)

4. Actions and Recommendations (A/R) Summary, p. 58; "The National Strategy to Secure Cyberspace" URL: http://www.whitehouse.gov/pcipb/appendix.pdf (29 Sept 2004)

5. Ward, David. "Letter to Presidents Regarding Cybersecurity" Eye on Washington, 28 Feb 2003 URL: http://www.acenet.edu/washington/letters/2003/03march/cyber.cfm (29 Sept 2004)

6. Cole, Eric. Hackers Beware, p. 18. Indiana: New Riders Publishing, 2002.

7. SANS GSEC Security Essentials Training Materials, Defense-in-Depth, Book 1-2, p. 15, SANS Institute, v2.2, 2004

8. MacInTouch Reader, Reports, "Opener Malware", 22 Oct 2004 URL: http://www.macintouch.com/opener.html#oct22 (27 Oct 2004)

9. K-OTik Security Research and Survey Team, "K-OTik-Fedorah-Redhat Fake Security Alert / Trojan Source Code & Analysis", 25 Oct 2004 URL: http://www.k-otik.com/news/FakeRedhatPatchAnalysis.txt (28 Oct 2004)

10. mi2g, News Alert, "Deep study: The world's safest computing environment", 2 Nov 2004 URL: http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/021104.php (20 Dec 2004)

11. SANS Institute, "About the SANS Institute", SANS Press Room © 2002 – 2004 URL: http://www.sans.org/aboutsans.php (9 Nov 2004)

12. SANS CDI East 2004, " Security 309: Intro to information Security (Track 9), 9 Nov 2004 URL: http://www.sans.org/cdieast04/description.php?tid=137 (9 Nov 2004)

© SANS Institute 2005 Author retains full rights.

13. SANS CDI East 2004, "Management 414: SANS®+S™ Training Program for the CISSP® Certification Exam (Track 14)", 9 Nov 2004 URL: http://www.sans.org/cdieast04/description.php?tid=135 (9 Nov 2004)

14. SANS CDI East 2004, "Management 512: SANS Security Leadership Essentials for Managers (Track 12), 9 Nov 2004 URL: http://www.sans.org/cdieast04/description.php?tid=133 (9 Nov 2004)

15. HSARPA, Homeland Security Advanced Research Projects Agency, Solicitations and Teaming Portal, 19 Oct 2004 URL: http://www.hsarpabaa.com/main/homepage.htm (10 Nov 2004)

16. BAA 04-17, Cyber Security Research and Development, Proposer Information Pamphlet, 9 Sept 2004 URL: http://www.hsarpabaa.com/Solicitations/CyberBAA_0908_FINAL.pdf (10 Nov 2004)

17. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), 16 Sept 2004 URL: http://www.cms.hhs.gov/hipaa (23 Nov 2004)

18. Family Educational Rights and Privacy Act (FERPA) – 20 U.S.C. § 1232g; 34 CFR Part 99 URL: http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html (23 Nov 2004)

19. Federal Trade Commission – Facts For Businesses, "Financial Institutions and Customer Data: Complying with the Safeguards Rule" URL: http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm (26 Mar 2003)

20. The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (P.L. 107 – 188), National Conference of State Legislatures, Overview of grants for states and local governments URL: http://www.ncsl.org/statefed/health/pl107-188overview.htm (23 Nov 2004)

21. McCarthy, Jack. "Sarbanes-Oxley: How Will it Affect NonProfits and Higher Education Institutions? An Interview with Jack McCarthy and John Mattie", PwCglobal.com Business Archive July 2004, PricewaterhouseCoopers © 2002 URL: http://www.pwcglobal.com/extweb/newcolth.nsf/docid/08f02b1b23d455e385256c9c00679322 (32 Nov 2004)

22. Mattie John. "Sarbanes-Oxley: How Will it Affect NonProfits and Higher Education Institutions? An Interview with Jack McCarthy and John Mattie", PwCglobal.com Business Archive July 2004, PricewaterhouseCoopers © 2002 URL: http://www.pwcglobal.com/extweb/newcolth.nsf/docid/08f02b1b23d455e385256c9c00679322 (32 Nov 2004)

© SANS Institute 2005 Author retains full rights.

23. MSN Money, "Safeguard your Social Security Number", Bankrate.com, 20 Aug 2004 URL: http://moneycentral.msn.com/content/banking/financialprivacy/P33718.asp (20 Aug 2004)

24. Netigy, SABSA®, Copyright © 2002, p. 1 URL: http://www.geocities.com/infosecpage/SecurityArchitecturePaper.pdf (5 Dec 2004)

25. Sherwood, John. Executive White Paper, "SABSA® Security Architecture", p. 1, Copyright © 2002 URL: http://www.geocities.com/infosecpage/SecurityArchitecturePaper.pdf (5 Dec 2004)

26. Sherwood, John. Executive White Paper, "SABSA® Security Architecture", p. 5, Copyright © 2002 URL: http://www.geocities.com/infosecpage/SecurityArchitecturePaper.pdf (5 Dec 2004)

27. EDUCAUSE, About EDUCAUSE, EDUCAUSE Home Page, 5 Dec 2004 URL: http://www.educause.edu/content.asp?page_id=720&bhcp=1 (5 Dec 2004)

28. EDUCAUSE Resources, 5 Dec 2004 URL: http://www.educause.edu/resources (5 Dec 2004)

29. UNISOG Home, 21 Dec 2004 URL: http://www.unisog.org (21 Dec 2004)

30. The Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860, 28 Oct 1998; U.S. Copyright Office Summary, p. 2, December 1998 URL: http://www.copyright.gov/legislation/dmca.pdf (5 Dec 2004)

31. The Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860, 28 Oct 1998; U.S. Copyright Office Summary, p. 4, December 1998 URL: http://www.copyright.gov/legislation/dmca.pdf (5 Dec 2004)

32. Yahoo! News Australia & NZ, Variety, "Music Biz to Give File Sharers Amnesty" 5 September 2004 URL: http://au.news.yahoo.com/030904/11/lkfp.html (13 Dec 2004)

33. Sturgeon, Will. "Will 'bounty' scheme stop spammers?", silicon.com, 17 Sept 2004 URL: http://www.silicon.com/research/specialreports/thespamreport/0,39025001,39124098,00.htm (22 Sept 2004)

© SANS Institute 2005 Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**