Improving Higher Education Information Security: Focus on the IT department

Stephen Reeder

May 23, 2002

Certification: GSEC v.1.4 Option 1

Abstract

The protection of technology assets is a major concern at many universities today. But years of poor information security practices cannot be corrected over night. At many institutions of higher education enterprise-wide defensive strategies are generally lacking if they even exist. New efforts to move to an improved level of security are not easy and don't happen quickly. But those who would do harm to important assets are constantly on the prowl for their next exploit. So, what does a university do to protect its assets in the absence of enterprise-wide strategic plans and actions for information security? The answer is that Senior IT management can still significantly improve the security posture of the institution by focusing security efforts within the central IT department. Even so, there are many challenges that must be overcome. This paper looks at obstacles that may stand in the way of securing the IT department systems, some basic reasons good security practices are needed, practical steps that can be taken to improve security, a discussion of mistakes that are easy to make when implementing security solutions, and the need to increase security for the purpose of revenue generation.

Introduction

Mark Twain once said, "Everybody is talking about the weather but nobody does anything about it." Using the context of information security instead of weather, his statement seems to describe the state of information security efforts in many organizations. But nowhere are information security deficiencies more pervasive than at institutions of higher education. Cultural and political factors at colleges and universities create a difficult and complex setting to enact change of any kind. Also, the mission (emphasis on teaching and learning[1]) at academic institutions is fundamentally different than that of profit-driven corporations. Because of these factors the balance between the information security pillars of confidentiality, integrity, and availability in higher educational environments is tipped towards availability. This is due to the implicit emphasis on openness (availability). Despite this constraint it is still possible for universities to implement effective information security programs. But there currently seems to be few institutions with comprehensive enterprise-wide security plans and programs in place. Creating such plans and programs takes considerable time, effort, and requires sufficient resources to implement. So, what can be done to protect critical institutional assets and improve the organization security posture in the absence of a comprehensive program? The answer is that Senior IT management can still significantly improve the security posture of the institution by focusing security efforts within their area of control, the central IT department.

Challenges

The IT department may or may not own, control or maintain all of the institution technology equipment (server systems and network and telecommunications infrastructure equipment). But the IT department normally does own, control or maintain the most critical technology equipment. Even so, there can be considerable obstacles to increasing security on these systems.

First, it is not likely that the IT department can mandate new or modified security policies on their systems since many different constituencies may use them. This means there must be collaboration with faculty, department staff and students. In addition, in order to enact policy changes the General Counsel and senior executive administrators may need to be involved. Each group has specific needs that may make the process of enacting broad new or modified policies difficult, lengthy and cumbersome.

Second, the existing technical infrastructure can be an impediment if it is outdated or poorly designed. Security solutions need flexibility in order to implement different solutions for different groups. For example, a poorly designed network may prevent student residence hall users from being segmented from the rest of the network. This type of design not only can cause network congestion problems for the entire campus network, but also increases the risk of unauthorized network access to critical systems.

Third, obtaining sufficient resources for security will always be problematic. It is no secret that most IT departments believe their budgets and staff are already overextended. The addition of security responsibilities increases senior IT management's responsibility to place a higher emphasis on setting priorities for staff.

Lastly, many IT departments seem to function only in a reactive mode when it comes to information security measures. They traditionally respond to circumstances that could have been avoided rather than take the necessary preventive actions. Good information security practices require planning for both reactive and proactive modes.[2] Examples of good proactive planning include creation of good security policies, and vulnerability testing and assessments. Examples of reactive planning may consist of Intrusion Detection Systems (IDS) and anti-virus software. In an environment where there is little proactive planning it usually takes a potential or actual catastrophe to focus attention on correcting security related problems. The trouble with reactive-only operations is that solutions to problems are focused on only what went wrong this time, not on a permanent solution that is prepared for different situations.

Importance of Information Security

Although the fore-mentioned challenges need to be addressed, there first needs to be a good understanding within the IT department of why good security practices are needed. Unfortunately, not all IT staff or management may understand the importance or significance of their part in keeping systems secure. They need to understand that academic institutions do have assets that can be compromised and that there are significant motivations for hackers to attack these systems.

Former U.S. Attorney General Janet Reno once said, when referring to an enemy state, "They have computers and they may have other weapons of mass destruction." Her inadvertent correlation between computers and devastating weapons actually should be taken very seriously. Lax security measures can make university computers susceptible to Trojan Horse type of breeches. Systems that have been compromised in this manner may eventually be used to launch a network attack against government, emergency response, or other type of critical computer networks. It should be considered a patriotic duty to make the best effort possible to ensure that technology assets cannot be compromised and used as part of a distributed denial of service (DDoS) attack[3] on the critical infrastructure[4] of the country.

A related reason for emphasizing good security practices in the IT department is that compromised computers can be used to attack the computer networks of other companies or institutions. It's distressing enough when an organization has its own systems compromised. But it is especially serious and embarrassing when these systems are used to cause harm to other organizations. In today's litigious society there is a real possibility that lawsuits could be brought against organizations because of damage caused by their poor security practices.[5] At the very least, other organizations could decide to restrict access to and from the insecure network due to the unreliable security stance of its systems. This type of restriction could have detrimental effects on those who need to correspond and share information.

Not to be ignored is the actual threat to the internal network and data. Hackers have different motivations for performing their disreputable activities. Some are looking for ways to make personal gain by stealing personal information such as credit card numbers. Others simply want to inflict as much harm as possible by destroying data and operating systems. As previously mentioned, some hackers may simply want to use an organizations systems as a platform from which to attack others or to cause embarrassment, such as posting the organization payroll file on the Internet. But the end result of a successful attack is that systems are compromised, and cannot be trusted. Once this is discovered it takes considerable work to determine what has been compromised and how it should be restored to a secure state.

An additional concern is the possible financial impact of poor security. Institutional bond ratings or accreditation could be affected by lack of adequate security practices and policies. Year 2000 computer compliance efforts affected bond ratings so it should be expected that information security requirements would be included sooner or later.

Lastly, is the security level that will be mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[6] The regulations governing this new law are scheduled to go into effect in April of 2003. While not all final regulations have been issued, it can be assumed that institutions that have medical practices or handle patient information will need to meet some sort of minimal security levels in order to ensure privacy and comply with the law.

A Pragmatic Approach for the IT Department

The premise of this paper is that in the absence of a comprehensive institution wide information security plan the IT department can take steps within the department to improve the security posture of the institution. So, absent the institutional policies, resources, and possibly cooperation from others, how can the security posture be improved? [12]

First, the IT department head should make information security a top priority at all levels within the department and allocate available resources accordingly. This is the most important component. If top-level management doesn't understand the importance of improving security, and then take action, little will be accomplished. Next, IT management should adopt an information security strategy for the IT department. The strategy should be to assure the confidentiality, integrity and availability of all IT controlled or maintained systems (hardware, application software, and OS). Last, tactics should be employed to achieve the strategy. One commonly suggested tactic for implementing security strategy is a concept referred to as "defense in depth". This tactic involves enacting numerous layers of security protective measures (defensive measures for each layer of the OSI model) to reduce vulnerability. For example, security awareness training, physical access security improvements, perimeter devices such as network firewalls, and intrusion detection systems, are different layers of defense. In order to negotiate a successful attack, a hacker would need to make a concerted effort to defeat all of the defensive mechanisms (layers). Defense in depth can be implemented in the IT department even when resources are scarce because not all layers necessarily require new expenditures or need to be foolproof. Below are some reasonable steps that can be taken to create an IT department security plan and to add layers of protection:

1. The IT department head should appoint an information security team leader to oversee a coordinated effort within the IT department. The team leader does not need to be a highly technical person, but should be familiar with the IT department and institution, be organized, and possess good project management skills. The team

leader must also be empowered with the proper authority to attain cooperation within the department.

2. Require each sub-unit within the IT department to assign a capable staff member to work with the security team leader on the security team. It is important that IT department personnel are accountable for security and realize that they have a stake in good security practices.
3. Set up an IT dept. security incident response team (SIRT).[7] The team should determine how to coordinate incident reporting and response issues for the IT organization. Most organizations already have staff handling security incidents within their own individual sections of responsibility. But information compilation, review, and centralization of reporting are normally lacking. So, the goal is to have a central point of contact that can pull all the information together, analyze the information, provide management reports, and help avert future incidents.
4. Perform an assessment of the current state of security in the department.[8] The first thing the security team should do is to identify the assets that need to be protected and determine the current security state for each asset. From this assessment it can be determined what needs protection or restriction of access and gain a realistic view of the current security posture. This also provides a baseline from which to measure progress. The assessment task may be less difficult if security audit reports or vulnerability tests already exist.
5. Emphasize security awareness as one of the two most important and effective means of addressing information security.[9] It is important to remember that the weakest link in information security is people. The strongest security measures and technology can easily be circumvented by intentional or unintentional human failure to follow prescribed security practices. The most cost effective security practice that can be implemented is a security awareness program. Even if there are few resources available to enact a security program within the department, a good security awareness program can be developed. Training on security policies and procedures is an important part of any awareness program. But it may be difficult to provide training if the policies have not been developed by the institution or department. Because of the slow-to-change academic culture it may be difficult for the institution to quickly develop, change or enact policies. But the IT department can still hold itself to higher standards even if policies don’t exist institution wide. The security team should identify good policies, enforcement procedures and have the IT department head mandate that the IT department will adhere to them. Under this scenario the IT department will be an example to the rest of the organization and will be able to implement a good quality security awareness program within the IT department.
6. Emphasize disaster recovery and contingency planning processes as the other most important means of addressing info security.[10] There certainly is nothing new about the need for good recovery and business continuation processes. However, the potential for harm to computer systems and networks is greater than at any time in history. In addition, it is well known that there is no security solution or group of

solutions that can guarantee a totally secure environment. It is highly improbable that anyone would make a public claim to have a totally secure environment. Even if someone believed it to be true it is doubtful that they would be brave enough to make the claim public because of their fear that they could be wrong. In fact, hackers would probably compromise their systems in a very short time period. So, of all the things that could be done to protect systems there is nothing more important than being able to recover from an attack of system failure. To be able to recover from an attack is to still be in business. The inability to recover may translate to significant harm to the organization. The assumption should be that at some point there will be a need for a major recovery from some sort of incident or disaster. The disaster could be intentional, unintentional, or an act of God. Typically, disaster recovery and contingency planning are considered a "back burner" type of issue in many IT departments. Other projects seem to always have a higher priority and management often assumes that backup and recovery processes of critical data are happening and are reliable. For a university environment with many distributed servers and other devices, it is important to verify that backups and recovery systems are in place, are actually occurring, and are tested on a regular basis. Also, management may assume that if critical hardware is destroyed, new equipment can be acquired quickly. Maybe and maybe not. There needs to be contingency plans in place in case new systems cannot be obtained quickly. Every critical asset should have a recovery and contingency plan. However, be aware that disaster recovery and contingency planning efforts can become stalled because of the frustration associated with trying to identify every disaster that could possibly take place. It is a mistake to take this approach. In an article by Brian Fonseca [13], Alan Lloyd Paris is quoted as saying, "the idea is to plan around a particular set of outcomes, as opposed to planning for any particular emergency". Paris went on to say that "You can't plan for everything, so you have to develop a plan that's flexible and that takes a look at a tiered set of problems." Paris gives an example of this by stating, "rather than planning recovery based on certain external threats – such as a bomb, or a chemical or biological attack – use a simple triple-tiered approach: Plan what to do when building access is denied, what to do when a certain floor needed to transact business is closed and how to recover from a particular system outage." The task of reviewing or creating disaster recovery and contingency plans should fall to the IT security team. But make sure that the personnel that need to be involved with disaster recovery understand the plan and their responsibilities within the plan. Lastly, practice and improve the plan by staging mock incidents.

7. Identify and implement physical access and security improvements.[11] First, make sure access to computer rooms, telephone switch rooms, network equipment rooms and environmental control areas are limited to those people who have a legitimate need to do work there. This is one of the easiest actions that can be taken. But be aware that it may greatly irritate those who think they should have access for any reason they can concoct. The security team should identify someone to be appointed to oversee the

access restriction effort and to enforce the access rules. Be warned that changing people's habits is a difficult thing to do. In an environment where security has been historically lax, resistance to physical access changes should be expected. One critical element is that, if there isn't support from top management, enforcing access rules is nearly impossible. So, it is imperative to make sure there is solid management commitment to access restrictions and that the rules are clearly explained before implementation. Next, improve physical security by keeping doors to critical areas shut and locked. Personnel needing regular access to these areas to do their job should be assigned a key. All others should follow an established approval and logging procedure. If necessary, locks should be changed and management of the new keys should be tightly controlled. If possible, restrict access to the entire floor or hall that leads to the restricted areas. On the exterior of the premises, identify any obvious vulnerability and, at least, start the planning process for increasing protection. For example, there may be unsecured power shut off switches or air conditioner compressors. Failure of a telephone or computer room air conditioner, either through natural causes or sabotage, could cause a serious disruption of services.

8. Add security responsibility language to all IT department job descriptions. Although it may take some time to accomplish, every IT department staff should have a security responsibility statement within their job description. A simple example of such a statement for staff is: "Stay knowledgeable of, and abide by, established university and departmental information security standards, policies, and procedures."
9. Apply Defense-in-Breadth. An interesting concept that should also be considered is the "defense in breadth" tactic that builds upon defense in depth. Since there is no perfect security solution, any given defensive measure can be defeated given enough time and commitment. Employing many defensive mechanisms (highly effective or not so effective) at each layer will increase the overall probability of successful defense. In an article in Information Security Magazine[15] regarding the effectiveness of defense in breadth, Peter Tippett said, "If one control is 80 percent effective, then it fails one out of five times. Two controls, each 80 percent effective, together will fail one out of 25 times. Three 80 percent effective controls, operating together, will fail one out of 125 times. In other words, they will succeed with a likelihood of 99.2 percent." So, multiple less than 100% effective defensive measures can prove to be a very effective overall solution.

Mistakes That Are Easy To Make: Things Not To Do

Former Major League Baseball player Lawrence "Yogi" Berra once said, "You've got to be very careful if you don't know where you're going, because you might not get there." This apparently contradictory statement seems to describe the approach some organizations take in trying to secure their systems. Meaning, they don't really have an organized thoughtful plan, don't know what goal they are trying to reach, and end up spending resources inefficiently in implementing security mechanisms. With that thought in mind, there are some important things not to do when improving the IT department security.

- Don't try to implement security over systems you cannot control. Scott Blake, a security expert at Bindview Corporation stated to me in a correspondence, "The unsuccessful model is to try to provide security for everyone regardless of standards on the systems. This is simply too expensive to support." The bottom line here is not to support systems that don't adhere to security standards. It is simply too costly, time consuming and will meet with little success. Within the IT department all personnel should be required to abide by security standards. This will be more difficult to achieve outside the IT department.
- Don't start buying security solutions (equipment, software, services) without a well-conceived plan. For example, there has been much talk about implementing firewalls to protect internal network assets. But without policies to guide firewall access rules the firewall may be nearly useless. There is no limit to the amount of money that can be spent (or wasted) on security solutions. IT management needs to avoid the tendency to approach complex security problems with simplistic uninformed solutions. Since it is well known that there is no single security solution and organization security resources have limits, it is imperative to assess the security posture and develop an organized approach.
- Don't implement new technology (software or hardware) without a security plan. An example of this is wireless networking.[14] The wireless revolution is thundering down the tracks and the demand for more of this technology will continue to grow. Those organizations that do not develop security standards for implementing wireless systems will be putting their networks and organizations at great risk of being compromised. The same can be said for application software systems. Software developers (in house and vendors) should be required to abide by the security standards of the IT department. Evaluation of software (prior to purchase or implementation) should include security requirements.

Return on Investment

Unfortunately, it has been standard practice for many organizations to view information security expenditures as a resource draining activity. It is uncertain as to whether this perception has changed or will change in the near future. Even so, while information security efforts are necessary and are a cost of doing business, there can be a good return on investment. This is because universities are increasingly dependent upon revenue-generating programs such as distance learning, web registration, and other e-commerce type of applications. These revenue-generating activities are not possible without a good information security strategy and practices. Well-planned security programs provide the assurance that these transactions can take place in the safest manner possible and can benefit the organization by ensuring the continuance of operations and assistance with revenue enhancement.

Conclusion

At universities with little or no structure to their security efforts, the IT department has the responsibility to take the lead in protecting organization assets. The IT department can increase organization security by implementing its own security plan. This is not an easy task and there are many obstacles that can emerge to prevent progress. But the most important key for the IT department is to gain a solid commitment from top management to create an information security strategy for addressing technology asset protection. Once that commitment exists security planning efforts will have a high likelihood of success.

References

[1] Seattle University main web page. "Mission and History".
URL: http://www.seattleu.edu/about/mission.asp - TL

[2] Reavis, Jim. "Be Proactive In Your Security." SC Magazine. April 2002 (2002): 66.

[3] Conry-Murray, Andrew. "Swatting Persistent Security Pests." Network Magazine. December 5, 2001.
URL: http://www.networkmagazine.com/article/NMG20011203S0005

[4] Verton, Dan. "U.S. Readies Plan for Protecting Key Systems." Computerworld. March 18, 2002.

[5] Scalet, Sarah D. "See You In Court." CIO magazine. November 1, 2001.
URL: http://www.cio.com/archive/110101/court.html

[6] "HIPAA Final Privacy Rules." HRnext.com.
URL: http://www.hrnext.com/content/view.cfm?subs_articles_id=1859

[7] "Computer Security Incident Response Team (CSIRT) Frequently Asked Questions." Carnegie Mellon. CERT Coordination Center®.
URL: http://www.cert.org/csirts/csirt_faq.html

[8] HORSEMAN, SHERI. "How to conduct periodic self-assessments." Computerworld. May 03, 2001.
URL:

http://www.computerworld.com/securitytopics/security/story/0,10801,60172,00.html

[9] Peltier, Tom. " How to Build a Comprehensive Security Awareness Program." Computer Security Journal. Volume XVI, Number 2, 2000:23-32.

[10] "Getting Started: Disaster Recovery Planning, Without Destroying Your Budget." Disaster Recovery Yellow Pages ™.
URL: http://www.disasterplan.com/yellowpages/intro.html

[11] Armstrong, Illena. "Physical Security: Do You Have Enough?" SC Magazine. April 2002:38-41.

[12] Cunningham, Chris. "Cheap Tricks for Information Security." SC Magazine. April 2002 (2002): 27.

[13] Fonseca, Brian. "A matter of minutes." Computerworld. March 29, 2002.
URL:
http://www.computerworld.com/managementtopics/management/recovery/story/0,10801,69954,00.html

[14] FOX, PIMM. "No Wires, No Security, No Solution." Computerworld. April 08, 2002:.

[15] Tippett, Peter. "Defense-in-Breadth." Information Security Magazine. February, 2002 (2002): 22 – 23.