Information Technology Risk & Security Management Report

Southwestern College

100 College Street
Winfield, Kansas 67156-2443

Prepared by: Gerry Hamill, CISSP, MBA, MCSE

Visit Date: October 16, 2007

Summary

EIIA's IT Risk & Security Management Team performed an on-site visit on August 14, 2007 to review Southwestern College's critical information technology areas. The objective of the visit was to identify those areas that expose the College to potential loss and to provide suggestions for reducing these risk exposures. This is the first on-site visit performed by EIIA's IT Risk & Security Management Team for Southwestern College. There were a total of fifteen (15) recommendations placed on the report as a result of this first visit.

Scope of Visit

The scope of the visit included:

- Interview with Mr. Ben Lim, VP for Information Technology.
- Walk through and review of the server and telephone system rooms.
- Walk through and review of several wiring closets and computer labs.

Comments

The knowledge, dedication and experience of Mr. Lim clearly provide Southwestern College with the highest level of Information Technology required by the user community of faculty, staff and students. In order to maintain a high level of expertise, mandatory on-going training for all IT staff needs to be required. This requirement should be included as a part of their goals and their administrative/job performance review.

Since the IT Department organizational chart is flat, the concept of "job-rotation" is something that is currently unachievable. However, the IT staff has done an excellent job of reducing administrative costs and risks in support of the organizational flat structure. This can be seen in the following:

- Ghost is used for the rollout of workstations. This reduces the amount of time and administration required and provides a simple way of resetting the workstations at any time.
- When re-deploying systems, a physical sector to sector Ghosting is performed. If a unit is to be retired, physical destruction of the hard drive is performed.
- An anti-virus license is provided to users that do not have their own antivirus solution.
- The public access computers in the library utilize Deep Freeze which is an excellent method of securing and protecting the units without any administrative costs. If a problem occurs, the end-user simply reboots the computer and it returns back to its ready state.
- Laptops are provided to the students; this makes management and deployment much easier.

During my visit I addressed the current Kansas State Notification Law for disclosing personal information and how it is based on the residency of the users affected. Best practice would be to follow the California notification laws as these are the model for the other 37 states that currently have notification laws in place. I have included detailed information on Kansas' Notification Law as an addendum to this report.

An additional concern that we discussed was on peer-to-peer (P2P) file-sharing and how Southwestern College may be exposed by this type of illegal sharing. Information on this topic can be retrieved from these two excellent sources: http://www.campusdownloading.com and http://www.musicunited.org. I have included the following information provided by these websites as an addendum to this report:

- Steps to address the problem (Awareness, Education, Enforcement)
- Technology measures that can be implemented to reduce or eliminate the problem.
- What the Courts have to say about illegal uploading and downloading of music files.
- Legitimate online content services to provide as an alternative to illegal sites.

Southwestern College uses ConnectED to notify everyone in case of emergencies. This provides for up to six (6) phone numbers, one (1) e-mail message and one (1) text message per subscriber (student, staff and faculty). The system was tested when I was on-site and will be further evaluated and tested to verify that the community can be notified campus-wide in case of an emergency.

Recommendations

Category I recommendations pertain to deficiencies that present imminent loss potentials, can be completed quickly, and do not involve significant capital expenditures to complete. These recommendations should be completed as soon as possible.

16/10-1 Backup & Recovery systems do not fully satisfy the needs for Disaster Recovery / Business Continuity and the off-site tape rotation system needs to be better defined.

Southwestern College does not currently keeps copies of their backup tapes stored off-site. The policy for tape retention and an incident response plan needs to be documented, and then tested. This process needs to include the IT experience and leadership of Mr. Lim in conjunction with the Business Office to determine the backup window to keep off-site and the methods for deployment. **Category I**

COMMENT: As part of the business continuity and disaster recovery plans, off-site tape management needs to be better documented and properly implemented. This process includes the identification of systems that need to be backed up regularly, where the tapes will be stored securely, who is allowed to access the tapes, and the method for transferring the tapes.

In addition to storing the tapes off-site securely, CD copies of all operating systems, applications, device drivers, patches and paper copies of all valid license codes should be created and stored with the tapes. These should be updated as the production systems change.

All current systems need to be ranked to identify the most critical systems and include the order and time required for recovery.

16/10-2 A policy for IT to monitor a user's e-mail needs to be created and enforced properly.

Southwestern College does not have a formal policy on monitoring e-mail, including reviewing or searching a users' mailbox for content. **Category I**

COMMENT: Users which include faculty, staff and students are often unaware of what is their personal property or fully understand their expectations of privacy. Southwestern College needs to develop a policy and update the user community on acceptable practices with e-mail. Within the policy, who is allowed to authorize IT to access a users' mailbox and when needs to be detailed. As with any warrant for search, the information that is being searched for needs to be identified before conducting the search.

16/10-3 A policy for user account passwords, including changing, length or lockouts needs to be created and enforced properly. Users including faculty, staff and students, can currently have their passwords reset by telephone if they have the required information.

Southwestern College does not have a formal policy on password management, including aging, uniqueness and resets. Additional considerations should be implemented to better secure the user accounts. **Category I**

COMMENT: Southwestern College utilizes Microsoft's Active Directory for authentication and can take advantage of Group Policies to enforce a system wide policy to address password exposures. Best practice is to force passwords change at a least once every semester, and for all users to be required to visit the IT support center if they lose their password. Clearly, staff and faculty need to be required to visit the IT support center if they need their password reset. However, based on the amount of risk that Southwestern College is willing to accept, the exposure of student accounts needs to be discussed and evaluated to determine what information would be compromised.

Best practices for Southwestern College would be to follow these standards:

- All passwords must have a minimum of 8 characters and contain a mix of both alphabetic and non-alphabetic characters.
- Passwords used must not be a word found in a dictionary.
- Passwords must not be sent through email in plain text.
- Passwords must not be stored in plain text on any electronic media.
- All vendor supplied default passwords must be changed.
- Passwords must never be disclosed via voice telephone or cellular lines.
- Faculty, staff and students must show up in person and present proper identification before obtaining a new or changed password.

I distributed a handout to Mr. Lim on EIIA's best practice for passwords and included a copy as an addendum to this report.

16/10-4 A better understanding of room access (Key Management) needs to be documented and implemented.

Southwestern College does not have a formal policy on management of keys to access critical IT areas. **Category I**

COMMENT: In the campus tour, Mr. Lim did not have a key to access the phone system in the Student Center. However, the local contractor who provides repair maintenance on the digital TV and phone system does have a key. Southwestern College needs to develop a policy on who has keys and better document access to critical IT rooms.

16/10-5 Outbound internet traffic needs to be better managed.

Southwestern College permits valid types of inbound traffic to specific systems only, such as mail and web, but all outbound traffic is allowed. **Category I**

COMMENT: Internet traffic is much more than web access to other internet sites. In order to contain a possible exposure on a machine that resides on the Southwestern College network, outbound traffic needs to be restricted so that the workstation does not perform a malicious function. Certain viruses, worms or trojans can make a workstation act as a mail server using port 25, also known as Simple Mail Transport Protocol (SMTP). By blocking outbound SMTP, even if a machine is affected, the malicious work can not be performed. An evaluation of what outbound traffic is required needs to be performed by the IT Steering Committee and only those allowed need to be configured.

Category II recommendations pertain to housekeeping or maintenance deficiencies. These include the development of loss prevention programs designed to reduce the probability and severity of a loss. Completion of these recommendations should be obtainable within one year and may require some capital outlay.

16/10-6 Additional physical preventive access controls need to be implemented.

The server room and wiring closet for the main distribution frame (MDF) are located on the second floor as part of Ben's office. There is no security, no locked doors and no cameras anywhere to monitor access.

COMMENT: Southwestern College needs to better control the type of physical access to the critical areas of IT. The Data equipment will be moved to the basement of Admin Center, which has extensive work scheduled, including electric, wall security, door security with framing and access code using low voltage.

In reviewing the new location, the main areas of concern would be to address water concerns since the server room will now be in the basement. The equipment needs to be off the floor and preventative means need to be implemented to keep the water in pipes on floors above from flowing onto the equipment below. Moisture sensors should be installed on the floor and monitored 24/7/365.

Also, the Admin Center does not have fire suppression, but with the Server Room upgrade project, fire suppression for the Server Room needs to be implemented.

The low voltage for the door access will provide tighter controls over who accesses the Server Room and will also provide auditing capabilities. In the case of a lost card or access code, IT can easily disable the access on the lost card or the access code, which would not be the case in a traditional keyed environment.

Also, the use of a camera system recording to DVR for restricted and critical areas of IT should be investigated. In the case of a loss, the information gathered by the system would justify the implementation.

16/10-7 The Telephone System room has a high exposure to environmental conditions.

The Phone system is currently exposed to water from piping above. In the open room next to the main phone system, the monitor for the Digital TV and Cable has water all over it and Mr. Lim said there used to be a tarp over some of the equipment to protect it from water, but the tarp no longer exists. **Category II**

COMMENT: Mr. Lim stated that the Phone System is under warranty and maintenance with a local firm for all parts and labor. He will check on the signed contract to determine coverage in case of known water damage. However, even if the equipment and labor by the local firm will address any water damage loss, the down-time and loss of productivity would be significant.

16/10-8 Documentation of critical systems needs to be performed and added to the Disaster Recovery / Business Continuity process.

Currently, Southwestern College does not possess technical documentation on the infrastructure, wiring, IP scheme used, applications, servers or Active Directory design. **Category II**

COMMENT: Proper documentation provides a road map for Southwestern College to follow in case of a disaster. Critical systems can be prioritized and knowing what equipment performs what functions allows for this to be possible. In addition, the documentation needs to be accessible to the Business Office and located in a secure location.

16/10-9 Additional logical detective access controls need to be implemented.

Currently, Southwestern College does not efficiently evaluate their audit logs, conduct detailed system monitoring, or deploy an intrusion detection or deterrent system. It is possible for an intruder to obtain information without being detected. **Category II**

COMMENT: It is uncertain how many attacks, successful or not, Southwestern College has incurred over the past six months to a year. Tools are available which make log analysis relatively easy. However, when choosing what needs to be logged, make sure the following are valid:

- Log files must not be modifiable without a trace or record of such modification.
- The system administrator actions, events, modifications, and changes must be logged.
- All production applications must generate a log that shows every addition, modification, and deletion of information.
- All production applications must keep logs of users' activities and statistics related to those activities.
- All security relevant events must be logged.
- Logs must provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with security policies.
- All commands issued by users must be traceable to specific individuals via the use of comprehensive logs.

COMMENT: A penetration test should be conducted to further identify weaknesses in Internet, Intranet, Extranet, and VPN technologies. The results of this test should include the following:

- Discovery and footprint analysis
- Exploitation
- Physical Security Assessment
- Social Engineering
- Deliverable including recommendations for corrective action for the systemic problems which may help propagate these vulnerabilities throughout Southwestern College.

16/10-10 Formal business continuity and disaster recovery plans do not currently exist.

Currently, Southwestern College does have an IT Disaster Recovery plan, but it lacks additional details for business continuity and is not updated on a regular basis. **Category II**

COMMENT: The document needs to change as the production environment changes. In addition, the procedures to address the different types of disasters should be detailed within the document. These include natural and information related disasters.

Natural Disasters – Examples include:

- Collapsed Building
- Collapsed Ceiling
- Smoke
- Fire
- Water
- Air Conditioning
- Excessive Heat or Cold
- Electrical Surge

Information Disasters – Examples include:

- Hardware Failure
- Software Failure
- Data Integrity Failure
- Security Compromise

16/10-11 Formal IT training for staff and faculty does not exist.

Currently, Southwestern College does not have a policy for annual training of staff and faculty on IT security and acceptable computer usage. This would include proper ways to save files, e-mails, password management, etc …. **Category II**

COMMENT: Although students receive brief training when receiving their laptops, no training is provided for faculty and staff. Periodic re-enforcement training for faculty and staff will eliminate much of the carelessness that causes IT security incidents. To minimize this exposure, Southwestern College needs to implement an acceptable use policy for staff and faculty which includes formal training.

The IT steering committee should formulate the strategy for training existing faculty and staff. In the case of hiring, there needs to be an adequate amount of time for IT to properly equip and train the new faculty or staff member. This includes the basics for accessing the network and mail, as well as the IT security awareness training.

When a faculty or staff member is terminated, there needs to be a process in place so that IT can securely disable their access to sensitive and confidential information, as well as the retrieval of the physical equipment that they are using. The IT and Human Resources department need to work closely on this as there is significant exposure if this is not handled properly. Strong communications between Staff and Faculty within Southwestern College will better reduce this exposure.

16/10-12 An IT assessment/review of the current production system needs to be performed on a regular basis.

Southwestern College has not had an information security assessment performed to identify areas of concern within the network, including the infrastructure and servers. **Category II**

COMMENT: Assessment testing is meant to not only test for known vulnerabilities, but also for unknown weaknesses that exist in an environment. Just as network traffic and the contents of a system's memory are both transient, an assessment is also similarly transient. Assessments only evaluate an environment at a specific point in time. In the event an assessment shows the environment currently meets the institution's criteria for security that does not imply that security is permanent.

Security is the product of a number of events, most of which are time sensitive. A secure environment today, does not insure security tomorrow. Should an employee download a peer to peer music swapping program, a piece of spy ware, a weatherbot, or remotely access the institution from home or a cyber café with an infected or trojaned machine, the institution is immediately vulnerable and compromised. Thus, it would be an oversight to equate successful assessment results with true security.

Well conducted security assessments can help sharpen the focus of a computer security team. Security assessments can help educate and set policy. Security assessments can show progress against a goal, or conversely show a deterioration of the environment. An assessment should be a living document, revisited and updated on a regular basis.

The major factors that affect the "regular basis" are costs associated with conducting the assessments and the environment volatility.

I distributed a handout to Mr. Lim on EIIA's best practice for security assessments. This is an excellent template or guide to follow when deciding on whether or not to have a security assessment performed. In addition, I have included a copy as an addendum to this report.

16/10-13 A review of the telephone system grounding should be conducted and/or verified.

It is uncertain whether or not the phone system is properly grounded to be able to sustain damages caused by a lightning strike. **Category II**

COMMENT: In reviewing claims submitted by all member institutions, a frequent cause of loss is power surges from lightning strikes to improperly grounded telephone systems. A review of the grounding system for the telephone system should be conducted or the results from a previous study should be evaluated to determine if the system is properly protected to handle a lightning strike.

16/10-14 The infrastructure connectivity consists of 10 MB shared hubs which need to be replaced.

Shared hubs do not provide the necessary level of security and need to be replaced with switched ports. **Category II**

COMMENT: In reviewing the infrastructure, many of the components are 10 MB shared hubs, which do not provide the security and performance of switches. Packets can easily be reviewed or "sniffed" for content which compromises usernames, passwords and data files. The IT infrastructure budget needs to include 10/100/1000 switches to replace the antiquated 10 MB hubs.

16/10-15 Authentication can be compromised through the wireless network which consists of Cisco Aironet access points with no encryption.

When using wireless networks, encryption needs to be enabled. The encryption can be WEP or WPA, depending on the level of security required. **Category II**

COMMENT: Although Southwestern College utilizes MAC authentication for the wireless network which limits the workstations that are allowed to connect to the network, the data packets that are transferred to and from the workstations are not encrypted. As discussed with the 10 MB hubs, packets can easily be reviewed or "sniffed" for content which compromises usernames, passwords and data files. Southwestern College needs to modify the wireless access points and include encryption.

In addition to the wireless encryption issue, Southwestern College should review implementing an automated appliance, such as Cisco's Network Admission Control (NAC) Appliance (formerly Cisco Clean Access) to enforce security policy compliance on all devices seeking to access network computing resources. This would provide minimized network outages, enforcement of security policies and significant cost savings with automated device repairs and updates.

Category III recommendations pertain to deficiencies that would require major capital expenditures and/or time to complete. There is no timetable for completion of these items.

There are no Category III recommendations at this time.