Lack of Standard Local Area Network (LAN) Administrative and Security Guidelines

3. Finding:

University-wide policies, procedures. and standards regarding LAN administration have not been adopted.

The University currently has at least 268 LANs established at their Carbondale and Edwardsville campuses. The LANs operating systems, number of users accounts defined to each LAN, and primary usages vary by network. The degree of formality, the extent, and the effectiveness of LAN administrative procedures were also found to vary by network. This variance depended on the technical expertise of the LAN administrator and the commitment of the adminisrator to communicating and enforcing adequate controls.

As part of the University's move to a decentralized client server processing environment the responsibility for administration of the mainframe and University backbone servers has been assigned to Office of Information Technology (OIT) and administration of the Local Area Networks—(LANs) has been assigned to the LAN administrators. However, the responsibilities of the OIT Division and its relationship with the many LAN administrators and their responsibilities must be defined in additional detail.

In addition. as the University increases their use of LAN based applications, the level of security over data residing on the system should be monitored to ensure that appropriate security over programs and data residing on the LANs is established. Therefore, it becomes necessary to have adequate LAN policies and procedures established and enforced to ensure that the integrity of applications and databases residing on the networks is maintained.

Our review found that the University had not developed standards to ensure that LAN administrators consistently and adequately administered their individual networks.

University-wide policies, procedures, and standards regarding LAN administration, and an administrative oversight body to monitor compliance with these standards, needs to be developed to assure the University’s intellectual efforts and investment in technology is properly safeguarded.

The principles of good internal controls require that reasonable cost-effective procedures be implemented to ensure the integrity and security of information maintained on the University's LANs.

Without the implementation of consistent security controls and administrative procedures for all LANs, there is a greater risk that unauthorized access to University resources may be gained and data destroyed. Once LAN administration and security standards have been established, compliance with these standards must be monitored to ensure University's assets are. properly safeguarded.

Standardization of University LAN administrative and security guidelines has been delayed while the University consults with other entities undergoing similar shifts from the traditional, centralized processing environment to a distributive processing or hybrid environment. The University has formed committees and task forces to study various administrative control structures and to determine which would be most effective in managing the distributive client server processing environment. (Finding Code No. 95-3)

Recommendation:

We recommend the University establish a multiffunctional task force to draft LAN administration and monitoring standards including standard security guidelines to ensure security controls, both physical and logical, are adequately addressed on University LANs. The task force should consist of SIU-C and SIU-E representatives from Information Technology, SIU-E Academic Computing, Internal Audit, and Users. Once drafted, the standards should be approved by the Chancellor's Office and adopted for both campuses. The University should consider establishing and implementing the following minimum standards and security parameters where appropriate:

- Users should only be alIowed to log on to one workstation on a LAN at any given time;

- Unless a user requires 24 hour access to a LAN, time restrictions should be set to limit when the LAN can be accessed;

- Unique passwords should be required for all users including the SUPERVISOR ID and other IDs having supervisor equivalence. Within some environments, there may be some non-user accounts that need to be established with supervisory authorization rights that cannot by the nature of its usage have a password associated with it. LAN administrators should review the established accounts on their LAN and determine if security is adequate;

- Passwords should have a minimum length of 4 characters;

- Passwords should be changed at least every 35 days;

- The number of invalid access attempts should be limited to no more than 5 attempts; and

- The number of times a user can log onto a LAN after their password expires should be limited to no more than 3 attempts.

LAN administration standards should address the foIlowing areas:

- Technical qualifications of LAN administrators and their immediate supervisors, and the training required of those personnel not meeting the technical prerequisites;

- Backup procedures including definition of critical and non-criticaI data, backup internals, off-site locations, Disaster Recovery Plans and the breakdown of responsibilities for data recovery assigned to the user and the LAN adminiistrator.

- User orientation programs to ensure that all users have been instructed on their role in maintaining network security. Such programs should address the user's responsibilitiy for safeguarding their network password, physical safeguards such as locking their keyboard and the office door, backup techiques for the PC's hard drive, the" University's policies on software piracy and the privacy of electronic data, and infiormation on how computer viruses are spread; and

- Security administration procedures to limit access to authorized users. These controls should address pre-verification and post-verification procedures related to maintaining the authorized user database.

To accommodate the great divergency of LAN operating environments, the University standards will need to be broad in nature. It will be necessary for LAN administrate-m to draft detailed procedures tailored to their environments that comply with the broad University standards that have been adopted.

We also recommend an administrative oversight body be appointed to perform an initial review of the individual detailed LAN administrative and security procedures that. have been drafted. After completion of the initial review, the oversight body should continue to monitor LAN administration for compliance with the adopted University standards.

Response

Accepted.

The University agrees with the substance of the recommendation and will establish a task force to address the important control issues raised.