Minnesota State Colleges and Universities
Information System Security Review

Selected Scope Security Audit
As of June 24, 1997

August 1997

This document can be made available in alternative formats, such as large print, Braille, or audio tape, by calling 296-1727.

Financial Audit Division
Office of the Legislative Auditor
State of Minnesota

97-46

Centennial Office Building, Saint Paul, MN 55155 • 612/296-1727

STATE OF MINNESOTA
OFFICE OF THE LEGISLATIVE AUDITOR
CENTENNIAL BUILDING, 658 CEDAR STREET • ST. PAUL, MN 55155 • 612/296-4708 • TDD RELAY 612/297-5353
JAMES R. NOBLES, LEGISLATIVE AUDITOR

Senator Deanna Wiener, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. Morrie Anderson, Chancellor
Minnesota State Colleges and Universities

Members of the Minnesota State Colleges and Universities Board of Trustees

We have audited selected areas related to security over the Minnesota State Colleges and Universities' (MnSCU's) new computerized business systems, as further explained in Chapter 1. We emphasize that this has not been a complete audit of all MnSCU computer systems or data centers. Our audit scope focused on MnSCU's new business systems, collectively referred to as the Integrated Statewide Records System (ISRS). The following Summary highlights the specific audit objectives and our conclusions. We discuss these issues more fully in the individual chapters of this report.

We conducted our audit in accordance with generally accepted auditing standards and *Government Auditing Standards*, as issued by the Comptroller General of the United States. Those standards require that we obtain an understanding of management controls relevant to the audit. These standards also require that we design the audit to provide reasonable assurance that the Minnesota State Colleges and Universities complied with the provisions of laws, regulations, contracts, and grants that are significant to the audit. Management of MnSCU is responsible for establishing and maintaining the internal control structure and for compliance with applicable laws and regulations.

This report is intended for the information of the Legislative Audit Commission and the management of Minnesota State Colleges and Universities. This restriction is not intended to limit the distribution of this report, which was released as a public document on August 29, 1997.

James R. Nobles
Legislative Auditor

John Asmussen, CPA
Deputy Legislative Auditor

End of Fieldwork: June 24, 1997

Report Signed On: August 26, 1997

SUMMARY

State of Minnesota
Office of the Legislative Auditor
1st Floor Centennial Building
658 Cedar Street • St. Paul, MN 55155
(612)296-1727 • FAX (612)296-4712
TDD Relay: 1-800-627-3529
email: auditor@state.mn.us
URL: http://www.auditor.leg.state.mn.us

Minnesota State Colleges and Universities
Information System Security Review

Selected Scope Security Audit
As of June 24, 1997

Public Release Date: August 29, 1997 No. 97-46

Agency Background

Minnesota State Colleges and Universities (MnSCU) began operations on July 1, 1995. The new MnSCU system combined two state-level higher education systems, state universities and community colleges, that had previously existed as independent systems. It also incorporated a series of technical colleges into state government. In total, MnSCU now consists of 37 different institutions with 54 campus locations.

MnSCU is developing a collection of new computer systems to help institutions manage their business activities. This system development effort, referred to as the Integrated Statewide Records System (ISRS), began in early 1994 and is still underway. The ISRS is a massive system development project. When development is complete, the ISRS will contain at least 15 different modules that will support most campus business functions, including accounting, human resources, student registrations, financial aids, and student housing.

Selected Audit Areas and Conclusions

Our audit analyzed how MnSCU controls access to its new business systems and its critical business data. Every campus is now highly reliant on the integrity of the data in its institutional database. Therefore, MnSCU needs strong security controls to ensure the accuracy, consistency, reliability, and availability of this data. MnSCU also needs strong security controls to help protect data that is not available to the public and reduce each campus' exposure to fraud.

We found that every institution's critical business data is at risk because MnSCU data centers have serious security weaknesses. MnSCU needs to address these security weaknesses immediately to prevent a disastrous loss, unauthorized disclosure, or the corruption of critical business data. We raise concerns about access to the systems from unauthorized environments, ineffective procedures for managing user accounts, inadequate control over powerful system privileges and security groups, and ineffective security monitoring procedures.

Minnesota State Colleges and Universities
Information System Security Review

Table of Contents

Audit Participation

The following members of the Office of the Legislative Auditor prepared this report:

John Asmussen, CPA	Deputy Legislative Auditor
Claudia Gudvangen, CPA	Senior Audit Manager
Chris Buse, CPA, CISA	Director of Information Systems Audits
Dave Poliseno, CPA, CISA	Audit Director
Carl Otto, CPA, CISA	Team Leader

Exit Conference

We discussed the issues in this report with the following staff of the Minnesota State Colleges and Universities on August 15, 1997:

Laura King	Vice Chancellor - Chief Financial Officer
Gerry Rushenberg	Associate Vice Chancellor
Alan Finlayson	Director of System Accounting

Chapter 1. Introduction

Minnesota State Colleges and Universities (MnSCU) began operations on July 1, 1995. MnSCU combined two state-level higher education systems, state universities and community colleges, that had previously existed as independent systems. It also incorporated local technical colleges into state government. In total, MnSCU now consists of 37 different institutions with 54 campus locations.

MnSCU is developing a collection of new computer systems to help institutions manage their business activities. This system development effort, referred to as the Integrated Statewide Records System (ISRS), began in early 1994 and is still underway. The ISRS is a massive system development project. When development is complete, the ISRS will contain at least 15 different modules that will support most campus business functions, including accounting, human resources, student registrations, financial aid, and student housing. A description of each module and its current implementation status can be seen in Table 1-1.

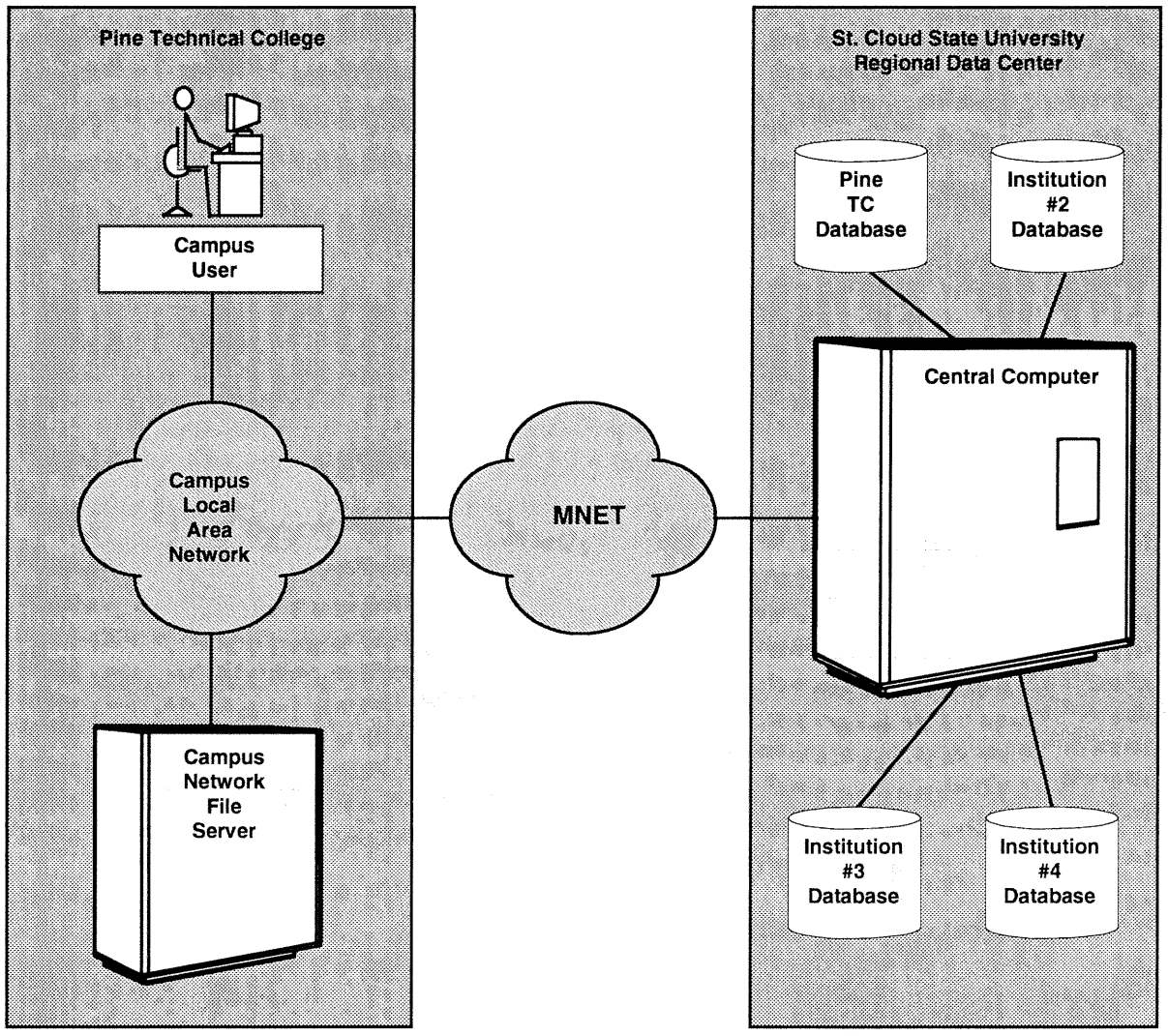
MnSCU is implementing its new business systems in a complex computing environment called "client server." Client server is a term for a special type of environment where several different computers work together to accomplish a task. Typically, these computers are connected and communicate over a high-speed local or wide area network. With all of the new ISRS modules, a campus user's personal computer (i.e. the client) completes a significant portion of the computer processing. The remaining processing occurs on a central computer at one of eight MnSCU data centers. Communications between campus machines and the central data center computers occur over the state of Minnesota's wide area network, commonly referred to as MNET.

Each institution stores its business data in its own database. MnSCU houses each institutional database at one of the eight data centers and connects them to the central computer at that site. This connection and the state of Minnesota's wide area network give campus users instantaneous access to their business data. Figure 1-1 shows an example of the key components of MnSCU's client server computing environment.

Table 1-1
Modules In the Integrated Statewide Records System (ISRS)

Module Name	Module Description	Implementation Status
MnSCU Accounting	Contains comprehensive accounting information for each college campus. Each campus has the ability to design its own chart of accounts and budget structure. A wide array of reports are available to help campuses manage their financial activities. It interacts with many other modules in the ISRS and with the state of Minnesota's centralized accounting system.	Currently Used By All Campuses
Human Resources	Supports most human resource management functions at college campuses. It helps campuses determine the amount to pay faculty and administrators on a biweekly basis. It also passes personnel data to the state of Minnesota's central payroll system where employee payroll warrants are generated.	Currently Used By All Campuses
Purchasing	Supports most purchasing functions at college campuses. Individual campus departments use it to requisition goods and process purchase orders. Planned enhancements will eventually let users record the receipt of goods and authorize payments to vendors.	Currently Used By All Campuses
Accounts Receivable	Helps college campuses manage amounts owed by students for housing and class registrations. Campuses can use it to send bills to students and record the subsequent collection of amounts owed.	Under Development
Financial Aid	Supports the awarding and disbursing of student financial aid. Edits and special programs help administrators comply with a wide array of complex state and federal regulations. It interacts with other state and federal student financial aid systems.	Under Development
Prospective Student/Applicant	Helps campuses identify prospective students and process new admission applications. It will also help campuses process admission applications for transfer students.	Under Development
Curriculum/Course Term	Helps campuses build a class schedule each term. It will interact with the college or university's master course catalog.	Under Development
Student Registration/Primary Student	Helps campuses manage the student registration process. It will also support many of the day-to-day activities of each campus' Records Office.	Under Development
Student Housing	Helps campuses manage student housing. It also will accumulate billing data for room assignments and food services.	Under Development
Placement Services	Helps support graduates or graduating students in their job searches.	Under Development
Student Payroll	Helps campuses manage their college work study programs. It lets departments or a campus business office enter hours worked and process the payroll. It also generates accounting transactions and student checks.	Under Development
Enrollment Management/ Communications	Helps campus manage student enrollment levels.	Under Development
Advising	Helps support student advising activities.	Under Development
Accounts Payable/ Checkwriter	Selects accounting transactions coded for check writing and produces checks on preprinted stock. It also helps campuses reconcile their local bank accounts.	Currently Used By All Campuses
Equipment/Fixed Assets	Records information about equipment and items susceptible to theft. It interacts with the accounting module to help campuses identify equipment and fixed assets that are missing from the inventory records.	Under Development

Figure 1-1
The MnSCU Client Server Computing Environment



Source: Auditor prepared.

As shown in the figure, Pine Technical College's database is located at the St. Cloud State University Regional Data Center. Pine Technical College is located in Pine City, Minnesota. The St. Cloud State University Regional Data Center services many MnSCU institutions in addition to Pine Technical College. Communications between each user's personal computer at Pine Technical College and the central data center computer occur over the state of Minnesota's wide area network, MNET.

Four of the MnSCU data centers service multiple institutions while the other four serve as stand-alone sites for individual campuses. Table 1-2 shows the location of each data center, the number of MnSCU institutional databases served, and the total number of campus users.

Table 1-2
Total Number of Databases and Users Served By Each MnSCU Data Center
As of May 13, 1997

Data Center Location	Total Number of Databases	Total Number of Campus Users
Moorhead State University	12	812
St. Cloud State University	9	571
Mankato State University	11	535
Metro Regional Computing Center (St. Paul, MN)	14	670
Metropolitan State University (St. Paul, MN)	1	230
Bemidji State University	1	253
Winona State University	1	229
Southwest State University (Marshall, MN)	1	203
Totals:	50	3,503

Source: Security data provided by MnSCU Information System personnel.

MnSCU uses security software to limit access to the various ISRS modules and the underlying institutional databases. However, by itself, specialized software cannot protect data from unauthorized use, modification, or destruction. Policies and procedures for system users are also necessary. Every campus is now highly reliant on the integrity of the data in its institutional database. Therefore, MnSCU needs strong security controls to ensure the accuracy, consistency, reliability, and availability of this data. MnSCU also needs strong security controls to help protect the data that is not available to the public and reduce each campus' exposure to fraud.

Our audit analyzed how MnSCU controls access to its new business systems and its critical business data. Chapter 2 discusses the specific scope of our audit and the conclusions that we reached. It also contains a series of audit findings and corresponding recommendations to improve controls.

Chapter 2. Controlling Access to Critical Business Data

Chapter Conclusions

Every institution's critical business data is at risk because MnSCU data centers have serious security weaknesses. MnSCU needs to address these security weaknesses immediately to prevent a disastrous loss, unauthorized disclosure, or the corruption of critical business data. We raise concerns about access to the systems from unauthorized environments, ineffective procedures for managing user accounts, inadequate control over powerful system privileges and security groups, and ineffective security monitoring procedures.

MnSCU purchased VAX computers, made by Digital Equipment Corporation, for each of its eight data centers. The operating system currently running on these computers, called OpenVMS, is also made by Digital Equipment Corporation. The OpenVMS operating system has a wide variety of security features. MnSCU uses some of these security features to control access to its business data and computing resources. However, MnSCU also developed some of its own custom security software.

Audit Objectives and Methodology

Our security audit focused on how MnSCU controls access to its new business systems and the underlying data. Specifically, we designed our work to answer the following questions:

- Does MnSCU have appropriate security administration procedures, and are those procedures consistently applied by employees at the eight data centers?

- Are MnSCU users limited to the minimum level of clearance necessary to complete their job responsibilities?

To answer these questions, we distributed a security administration survey to each of the eight MnSCU data centers. We then visited each data center to interview security administration employees and review their documentation. Finally, we gathered and analyzed extensive electronic security data from each data center.

Conclusions

MnSCU does not administer security from a central location, though a centralized structure is possible and often highly preferable. Instead, one or more individuals at each of the eight data centers enter security transactions and monitor system usage. We think these employees, working in a decentralized environment, are having a great deal of difficulty performing their

security administration duties. Most of these employees have many other responsibilities in addition to security administration. Most also have very little experience working with the OpenVMS operating system and have had only limited formal training. To compound this dilemma, MnSCU does not have written security policies or procedures for them to use as guidance.

In our opinion, MnSCU has inadequate security administration procedures at all of its data centers. As discussed in Finding 1, most users can alter or delete critical business data without using the intended ISRS business systems. As discussed in Finding 2, every MnSCU data center VAX has a large number of accounts that have either never been used or have been dormant for an extended period of time. Finding 3 discusses our concerns with the excessive use of powerful OpenVMS privileges. Finding 4 discusses weaknesses in MnSCU's procedures for creating, maintaining, and assigning users to security groups. In Finding 5, we discuss certain password weaknesses that came to our attention. Finding 6 discusses environmental control weaknesses. Finally, Finding 7 discusses problems with security monitoring at MnSCU data centers.

1. System users can alter or delete critical business data from uncontrolled environments.

Nearly all MnSCU data centers do not prohibit users from updating or deleting data without using the intended ISRS modules. MnSCU designed each ISRS screen with numerous edit programs. These edit programs are an extremely important control because they protect the integrity of the data that flows into each institutional database. Unfortunately, most users can circumvent these edits by updating or deleting data without using the appropriate ISRS screens. This is a very serious security weakness because it gives a large number of system users the ability to destroy entire institutional databases.

We investigated this problem and found it to be widespread. In fact, 49 of MnSCU's 50 institutional databases were vulnerable at the time of our audit. Most MnSCU security administrators were aware of this weakness. However, only one had taken the necessary steps to remedy the problem.

Recommendation

- *MnSCU should modify its security structure so that users cannot update or delete data from outside the intended ISRS screens.*

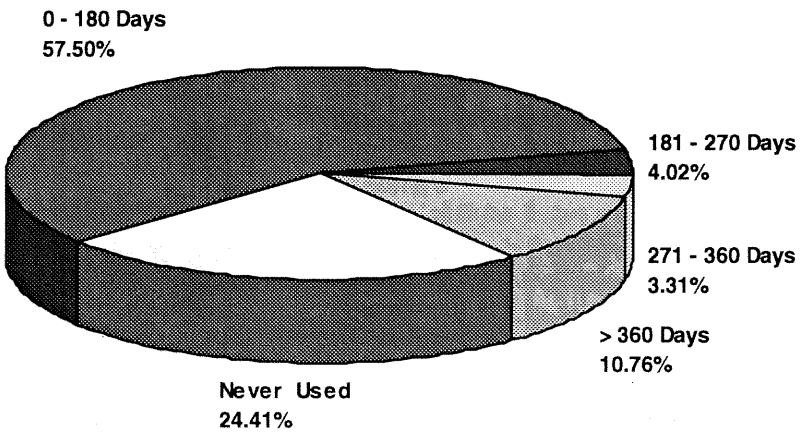
2. MnSCU does not have effective procedures for managing dormant user accounts at any of its eight data centers.

An extremely high percentage of the accounts on every MnSCU VAX computer have either been inactive for an extended period of time or have never been used at all. Controlling dormant accounts is a very important security administration responsibility. When left uncontrolled, dormant accounts can provide unauthorized users with easy access to computer resources and critical business data.

We analyzed account usage on all MnSCU VAX computers and found that the percentage of inactive accounts ranged from 27 percent to 57 percent. We classified an account as inactive if it had not been used for more than 180 days. Of particular concern, the percentage of accounts on each VAX that had never been used at all ranged from 15 percent to 37 percent. Many of these accounts had very high clearance because they were created for employees who work in the MnSCU System Office.

Figure 2-1 is an analysis of account activity for all eight MnSCU VAX computers. On average, approximately 42 percent of the accounts are inactive. Approximately 24 percent of the accounts on these computers have never been used.

Figure 2-1
Account Usage Analysis For All MnSCU VAX Computers
As of May 13, 1997



Note: Days indicate how many have lapsed since the account was last used.
Source: MnSCU security data.

Most security officers told us that they distribute user account lists to every campus on a periodic basis. However, none of the security officers removed dormant accounts without the prior approval of campuses. None of the security officers that we interviewed had automated tools to help them identify accounts that were dormant or had never been used.

Recommendation

- *MnSCU should develop procedures for disabling and removing accounts that are dormant or have never been used.*

3. MnSCU has inadequate controls over powerful OpenVMS privileges.

An excessive number of accounts on the MnSCU VAX computers have extremely powerful privileges. The OpenVMS operating system has 39 different privileges. Most users only need three of these privileges to effectively use the new ISRS business systems. Many of the remaining privileges are very powerful because they give users the ability to control the operating system, storage units, and system devices. Some OpenVMS privileges even give users the ability to completely bypass system security.

We found too many accounts that held one or more of the 14 most powerful OpenVMS privileges. These privileges present the most significant risks because if used inappropriately, they could result in the loss or destruction of data or the audit trail. Nearly every MnSCU data center had some highly privileged accounts that were no longer used. In most cases, these accounts were not disabled to prevent unauthorized users from gaining access. At one data center, we found 26 different accounts that had clearance to completely bypass system security. Some of these accounts belonged to consultants and other employees who were no longer working for MnSCU.

Most security administrators told us that they did not understand the functionality provided by each OpenVMS privilege. Therefore, they could not explain why specific accounts needed to have powerful privileges. We think that many of the accounts that currently hold powerful privileges may not need them at all.

Recommendations

- *MnSCU should provide its security administrators with OpenVMS security training so that they can make more informed security decisions.*

- *MnSCU should limit the use of powerful privileges to only those accounts that need them to perform specific job duties.*

4. MnSCU does not have effective controls over security groups.

MnSCU's procedures for creating, maintaining, and assigning users to security groups have serious weaknesses. MnSCU designs security groups for each of its new ISRS business systems. Each security group gives users access to a predefined set of computer screens. Security groups are very important because they provide the necessary foundation to separate incompatible business functions. MnSCU's security groups can limit each user to their own institutional database. They also can limit each user to the specific computer resources and data that they need to fulfill their job responsibilities. Unfortunately, serious internal control weaknesses are diminishing the effectiveness of MnSCU's security groups.

MnSCU does not have an employee who is responsible for managing security groups for the system as a whole. MnSCU also does not have a central repository for all of its security

documentation. We feel that these coordination and documentation weaknesses have contributed to the development of conflicting and redundant security groups. MnSCU has system development teams design security groups for each new ISRS business system. This approach is risky because the security groups for the ISRS business systems are highly interrelated. In fact, security group additions and changes made for one system may have unanticipated effects on the security of other systems. We analyzed the security group infrastructure for each VAX computer and found significant differences. Some security administrators told us that they needed to change the standard security groups because they did not work properly. Some even created their own security groups as a last ditch effort to give users access. We think that MnSCU needs to place greater emphasis on controlling security groups. Specifically, someone should be responsible for security group development, documentation, and maintenance. Strong controls over the movement of security group changes into the production environments also are needed. Currently, a large number of users have clearance to modify MnSCU's security groups on the eight data center VAX computers. This is due in part to the excessive use of powerful OpenVMS privileges.

MnSCU's procedures for assigning users to security groups also have significant weaknesses. MnSCU designed a standard system access request form for each of its new business systems. Each form contains a list of the security groups developed for the particular system. After selecting the appropriate security groups, certain campus or system office managers must approve the access requests. Data center security administrators then enter the appropriate security transactions. We reviewed this process in detail with security administrators and found a number of internal control weaknesses. Of greatest significance, some data centers do not take steps to verify the authenticity of the people who approve system access requests. We also found instances where MnSCU created new security groups or changed existing groups, but did not modify the standard system access request forms. Security administrators also told us that many campuses have difficulty understanding the functionality provided by each security group because the access request forms are not descriptive. In fact, for some systems we were unable to locate any external documentation describing the access provided by each group. Finally, security administrators told us that MnSCU does not notify all campuses after making security group additions or changes. Therefore, many campuses submit system access requests on outdated forms.

MnSCU does not have security clearance standards for any of its job positions. MnSCU also has not documented the potentially incompatible security groups for each new business system. Without this information, employees who complete and approve system access requests may have difficulty making informed decisions. Security administrators also have difficulty judging the reasonableness of access requests. These risks are compounded in an evolving computer environment, such as MnSCU's. Employees who request or approve access to a new business system may only have a limited understanding of the system's capabilities

We examined the security clearances for all MnSCU employees and found many serious weaknesses. These weaknesses went undetected by MnSCU. No one scrutinized security clearances for the system as a whole, and several problems with security clearances are apparent when comparing patterns between data centers. To illustrate, one data center gave over 50 percent of its users rights to a powerful security group that lets them change a college's chart of accounts. This is a critical accounting function that very few users should have the ability to

perform. We also found a large number of users with incompatible security clearances. For example, there were 287 accounts that could perform both payroll and personnel functions on MnSCU's new human resource system. Many of these users also had very high clearance on the state of Minnesota's payroll system where checks are produced. We also found 154 accounts that have clearance to both print checks and perform automated bank reconciliation functions. We even found one data center that gave a single user rights to every security group for all MnSCU business systems.

Recommendations

- *MnSCU should designate an individual or individuals to be responsible for overseeing all security group development, documentation, and maintenance. MnSCU also should only let certain designated individuals move security group additions or changes into production environments. Finally, MnSCU should secure its production security groups so that they cannot be modified by unauthorized users.*
- *MnSCU should create a central repository for all of its security group documentation. At a minimum, this repository should include current access request forms for every business system. It also should contain documentation that outlines the functionality of every MnSCU security group.*
- *MnSCU should ensure that all system access requests are properly authenticated.*
- *MnSCU should develop baseline security standards for job positions and document potentially incompatible security groups.*
- *MnSCU should scrutinize security clearances for the system as a whole and investigate the incompatible clearances that currently exist.*

5. MnSCU has weak password controls over some accounts.

We examined all MnSCU accounts and found 50 accounts where users are not required to change their passwords. We also found some accounts that security officers told us were shared by more than one user. Many of these accounts with weak controls belong to or are used by information system professionals with extremely high security clearances. Unique logon IDs and passwords are one of the most important controls in a computerized environment. When users share passwords, it becomes extremely difficult to trace actions to specific individuals. Allowing users to retain the same password indefinitely makes their accounts much more susceptible to compromise.

Recommendations

- *MnSCU should prohibit users from sharing passwords.*
- *MnSCU should require all users to change their passwords on a periodic basis.*

6. Most MnSCU data centers do not place environmental controls on user accounts.

Most MnSCU data centers are not taking advantage of OpenVMS' environmental security features. Environmental controls can limit user access attempts to certain days of the week or to specific time periods. They also can restrict each user to certain access methods, such as connecting to the system through a local network, a wide area network, or through a telephone line and modem. Environmental controls are very easy to implement and are normally transparent to legitimate system users. However, they are extremely important because they significantly reduce the opportunities available to computer hackers.

Recommendation

- *MnSCU should place environmental controls on user accounts whenever possible.*

7. Some MnSCU data centers do not have effective security monitoring procedures.

Some MnSCU data centers do not review security reports on a daily basis. Therefore, attempts to compromise the new business systems or institutional databases could occur and remain undetected. The OpenVMS operating system has a wide variety of tools and reports to help security administrators prevent and detect inappropriate activities. Customizing these tools and reports to meet the particular needs of MnSCU is a very important security administration responsibility. Monitoring security reports on a continuous basis is also critical. We reviewed security monitoring procedures and feel that many MnSCU data centers are not fulfilling these important responsibilities.

Some security administrators told us that they did not have time to review security reports each day. Some also told us that they had difficulty understanding the information in the standard OpenVMS security reports because they had no formal training. Most of the data center security reports that we reviewed only included the default information provided by the OpenVMS operating system. We saw very little security report customization at any of the MnSCU data centers. To improve controls, we feel that MnSCU needs to provide its security administrators with formal OpenVMS security training. Formal training will help them understand how to use the OpenVMS tools to customize their security environment. It will also help them understand the significance of information in their OpenVMS security reports.

Recommendation

- *MnSCU should develop custom security reports and monitor all security-related incidents on a daily basis.*

MnSCU

Minnesota State Colleges & Universities

August 25, 1997

Mr. James R. Nobles
Legislative Auditor
Office of the Legislative Auditor
Centennial Building
658 Cedar Street
St. Paul, Minnesota 55155

Dear Mr. Nobles:

Thank you for the opportunity to respond to the audit findings related to security of the new business systems being implemented by Minnesota State Colleges and Universities (MnSCU). We agree with all the findings, and have either taken action or are planning changes to implement the audit recommendations.

All of the new systems in use by the 53 MnSCU campuses have been developed since the July 1, 1995 merger of the community colleges, technical colleges and state universities. After a rapid start, the basic business systems - accounting, human resources, payroll and purchasing - are now beginning to stabilize. MnSCU is no longer simultaneously developing and doing business on the new business systems. The development phase is essentially complete, users have become familiar with the software, requested modifications are being implemented and support personnel are becoming skilled in the operation of the new equipment and customized software.

The audit raises substantial concerns regarding the risks present in the decentralized MnSCU information systems operating environment. Eight regional computer centers enable MnSCU to spread computing power across the state. While your audit found no evidence of actual data or system integrity breaches at any of the centers, it also highlighted the management challenges present in the current MnSCU computer center structure.

The chancellor has recently approved a restructuring of the reporting relationships for employees operating and developing the MnSCU management information systems (MIS). Currently, the vast majority of MIS personnel report directly to campus administrators and not to the MnSCU central administration. Many of the campus staff work on systemwide projects, serving both their home campus and the system office. A change to this arrangement will include the formation of a new structure with direct reporting of computer and other systemwide operations to the MnSCU Vice Chancellor - Chief Financial Officer.

Outlined below are the findings and a summary of the actions taken. We appreciate the assistance provided by your staff and look forward to continued input as we develop and refine the MnSCU Integrated Statewide Record System (ISRS).

550 Cedar Street St. Paul, Minnesota 55101
612.296.8012 Facsimile 612.297.5550 TDD 612.282.2660

1. **Recommendation: MnSCU should modify its security structure so that users cannot update or delete data from outside the intended ISRS screens.**

   Response: Effective August 19, 1997 the security structure was modified to allow users access to data from only the computer screens and standard reports. The ability to directly access data from outside the screens or reports will be retained by a handful of programers, system managers and developers. In the future, a small group of research personnel may be allowed direct access, but only in read-only mode. Mr. Gerry Rushenberg, associate vice chancellor for MIS, is responsible for implementing this recommendation.

2. **Recommendation: MnSCU should develop procedures for disabling and removing accounts that have been dormant or have never been used.**

   Response: Effective August 29, 1997 a procedure will be implemented to delete dormant and/or unused accounts after 45 days without activity. Mr. Dale Jarrell, director of MIS operations, is responsible for implementing this recommendation.

3a. **Recommendation: MnSCU should provide its security administrators with Open VMS security training so that they can make more informed security decisions.**

   Response: The recommended training will be scheduled for September 1997. Mr. Jarrell is responsible for implementing this recommendation.

3b. **Recommendation: MnSCU should limit the use of powerful privileges to only those accounts that need them to perform specific job duties.**

   Response: Privileges assigned to all users are being reviewed. The use of power privileges will be reviewed and restricted only to those users who need them. Mr. Jarrell is responsible for implementing this recommendation by September 15, 1997.

4a. **Recommendation: MnSCU should designate an individual or individuals to be responsible for overseeing all security group development, documentation and maintenance. MnSCU should also only let certain designated individuals move security group additions into production environments. Finally, MnSCU should secure its production security groups so that they cannot be modified by unauthorized users.**

   Response: A procedure has been put into production to ensure that the security groups cannot be modified by unauthorized users. The balance of this recommendation will be implemented by September 30, 1997. Ms. Cindy Trudeau, director of software maintenance, has been designated to oversee all security group functions.

4b. **Recommendation: MnSCU should create a central repository for all of its security group documentation. At a minimum, this repository should include current access request forms for every business system. It also should contain documentation that outlines the functionality of every MnSCU security group.**

Response: Ms. Trudeau has been designated to establish a central repository for security group documentation and functionality by September 30, 1997.

4c. **Recommendation: MnSCU should ensure that all system access requests are properly authenticated.**

Response: MnSCU will either develop a new software application or purchase software to manage and authenticate user requests to access the system. Mr. Jarrell is responsible for implementing this recommendation by September 30, 1997.

4d. **Recommendation: MnSCU should develop baseline security standards for job positions and document potentially incomparable security groups.**

Response: The MnSCU finance, human relations, student affairs and MIS departments will begin working to document the relationships between system security and job responsibility. Mr. Rushenberg is responsible for implementing this recommendation by December 31, 1997.

4e. **Recommendation: MnSCU should scrutinize security clearance for the system as a whole and investigate the incomparable clearances that currently exist.**

Response: We agree with the recommendation. Mr. Jarrell is responsible for implementing this recommendation by October 15, 1997.

5a. **Recommendation: MnSCU should prohibit users from sharing passwords**.

Response: Mr. Jarrell will distribute a systemwide MIS procedure by August 30, 1997 informing users that passwords may not be shared.

5b. **Recommendation: MnSCU should require all users to change their passwords on a periodic basis (90 days).**

Response: Mr. Jarrell will implement a systemwide MIS procedure by August 30, 1997 to require that all passwords be changed every 90 days.

6. **Recommendation: MnSCU should place environmental controls on users accounts whenever possible.**

Response: Mr. Jarrell will implement Open VMS environmental controls by October 15, 1997.

7. **Recommendation: MnSCU should develop custom security reports and monitor all security-related incidents on a daily basis.**

   Response: Mr. Rushenberg will develop and implement daily security reports by September 30, 1997.

Sincerely,

Laura M. King
Vice Chancellor - Chief Financial Officer

cc: Chancellor Morris J. Anderson