FINAL REPORT

OFFICE OF INTERNAL AUDITING

Minnesota State Colleges and Universities

MnSCU Network Security

Public Release Date: February 21, 2001

Minnesota State Colleges & Universities

Honorable Mary Choate, Chair
MnSCU Audit Committee

Members of the MnSCU Board of Trustees

Chancellor Morris Anderson

MnSCU Presidents

MnSCU has ambitious plans to expand the use of instructional technology and explore e-commerce applications. It would be a serious mistake, however, to pursue these opportunities without establishing a secure and stable information technology network structure. The risk of corrupted or lost data and denial of service attacks is real and growing. This study examined the security of about 60 local area networks connected to the MnSCU wide area network. In this report, we offer a series of recommendations to trustees, the chancellor, and presidents to protect the organization's information technology resources from external attacks and internal sabotage.

We conducted this study in compliance with the *Institute of Internal Auditors: Standards for Professional Practice of Internal Auditing* and the *Information Systems Audit and Control Association: Standards for Information Systems Auditing.* We interviewed over 100 MnSCU employees that are responsible for information technology throughout the organization. We are grateful to these employees for their assistance.

Ms. Beth Buse, Deputy Director of Internal Auditing, with assistance from Ms. Jennifer Struemke, Regional Audit Coordinator, was responsible for the lead work on this project, including the design of interview questionnaires. Other Internal Auditing employees, as identified on page *iii*, also contributed significantly to this project. Finally, I would like to acknowledge the expert program assistance that we received from Mr. Michael Janke, System Director for Wide Area Network Services.

Sincerely,

/s/ John Asmussen

John Asmussen, CPA, CIA, CISA
Executive Director
Office of Internal Auditing

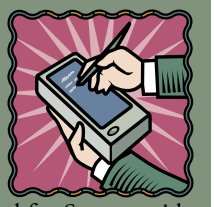
End of Fieldwork: November 30, 2000

500 World Trade Center • 30 East Seventh Street • Saint Paul, MN 55101
Phone 651-296-3471 • Fax 651-296-8488

CONTENTS

CHAPTER 1

The Threat is Real and Growing *page 1*



CHAPTER 2

The Need for System-wide Security Policies and Guidance *page 11*

CHAPTER 3

College & University Network Security Practices *page 25*

EXHIBITS

STUDY TEAM

The following representatives of the MnSCU Office of Internal Auditing contributed to the completion of this project:

Executive Director:	**John Asmussen, CPA, CIA, CISA**
Deputy Director:	**Beth Hammer Buse, CPA, CIA, CISA**
Lead Auditor:	**Jennifer Struemke, CPA** Regional Audit Coordinator West Metro Area
Regional Audit Coordinators:	**Tami Billing, CPA, CIA** Northwest Minnesota
	Marilyn Hansmann, CPA, CIA, CCSA Southeast Minnesota
	Kim McLaughlin, CPA Northeast Minnesota
	Paul Portz, CPA, MBA, CMA East Metro Area
	Melissa Primus, CPA, CIA Central Minnesota
Information Technology Audit Specialist:	**Eric Okpala, CPA, MBA, CISA**
Improvement Consultant:	**Julie Smendzuik-O'Brien, MPA, CQM**
Print & Web Designer, Layout & Production:	**Nancy Hoglund**

The office also recognizes the expert advice and guidance provided by:

System Director for the MnSCU Wide Area Network:	**Michael Janke**

MNSCU REVIEW & RESPONSE

Draft reports on network security or some specific sections of these draft reports were reviewed and discussed with the following members of the System Office and colleges and universities.

Morris Anderson	Chancellor
Dr. Linda Baer	Senior Vice Chancellor - Academic and Student Affairs
Laura King	Vice Chancellor - Chief Financial Officer
Bill Tschida	Vice Chancellor - Human Resources
Gail Olson	General Counsel
Dr. Penny Harris-Reynen	Board of Trustees Executive Director
Ken Niemi	Associate Vice Chancellor for Information Systems - Chief Information Officer
Dale Jarrell	Former Chief Technology Officer
Larry Simmons	System Director Software Development & Office of Security
Michael Janke	Director, Wide Area Network Services
Dr. Kathleen Nelson	President - Lake Superior College
Dr. Ron Thomas	President - Dakota County Technical College
Dr. Roy Saigo	President - St. Cloud State University
Dr. Tom Horak	President - Normandale Community College

Based on their review, the draft was modified to improve its clarity and accuracy. The final conclusions and recommendations represent the professional judgement of the MnSCU Office of Internal Auditing. Beginning on page v, is a letter from CIO Ken Niemi responding to this study.

Minnesota State Colleges & Universities

January 31, 2001

Mr. John Asmussen, Executive Director
MnSCU Office of Internal Auditing
30 East 7th Street, 500 World Trade Center
St. Paul, MN 55101

Dear Mr. Asmussen:

Subject: Response to the MnSCU Office of Internal Auditing Network Security Report

In a joint effort with my Information Technology Services management and staff, we have reviewed the Network Security Report and are in general agreement with the recommendations and findings. As you know, we have been developing a strong foundation for information technology security within the MnSCU system since the Year 2000 cutover. I have charged the Information Security Office with ensuring that significant, ongoing progress continues to occur in our management of information security. Recent progress includes adding new positions, reorganizing the responsibilities of existing staff, including significant changes in security procedures and functions in the four MnSCU Data Centers, and establishing procedures and formal relationships with campus security staff. We have created a charter for the Information Security Office that includes the responsibility for creating a comprehensive and integrated MnSCU security program making use of all available resources. As you are well aware, resources are scarce within the MnSCU system and it is often difficult to pull resources away from supporting the myriad business requirements of an integrated administrative system; we have no choice other than to leverage existing resources and postpone some important information system initiatives to make the improvements necessary in our information security management.

An essential part of the planned information security program is the Information Security Steering Committee, which will meet quarterly starting in February, 2001. The primary purpose of the committee is to review and recommend MnSCU information security policies, standards, and procedures. It will also address college and university network security policies, procedures and issues. ITS staff will lead and provide support to the committee. Committee membership will include representatives from the Office of Internal Auditing, the Infrastructure Steering Committee, and the Chief Information Officers of several campuses. Staff from the offices of the General Counsel and Human Resources will support the committee's efforts when addressing difficult human resource enforcement and data privacy issues.

We are currently in the process of leading the design of a common information technology planning process, including security planning, for all MnSCU institutions. This will be a flexible process designed to meet the varied and unique needs of all institutions and should support the strategic and tactical planning of ITS steering committees and the MnSCU IT Roundtable. The design process will start with the leadership and involvement of campus CIOs.

In order to meet potential emergency staffing requests from colleges and universities, particularly in response to security threats, the Information Technology Services division will collaborate with the campus CIOs to develop a process and a communication system to coordinate joint campus responses that leverage all MnSCU resources. Again, given the scarcity of available resources, an approach that builds on the teamwork of the central Information Technology Services and campus IT operations is critical.

As an overall guide to the development of MnSCU information security strategies, the Information Security Office is building the Information Security Program foundation based on the Control Objectives for Information and Related Technology (COBIT) framework. The British Standard BS7799 is another well-known framework for information security management. A successful security program could be built based on either of these standards; however, COBIT provides a more comprehensive framework, including a management guide very similar to a Baldrige systemic approach to continuous improvement. For this reason, we are adopting the COBIT framework for our security program. We will use BS7799 for technical guidance and possibly seek BS7799 certification in the future. The successful implementation of our information security program based on COBIT will ensure that MnSCU's information assets are protected against threats, which will continue to occur despite our most aggressive efforts, as you documented so well in your report.

Finally, significant improvement of information security within MnSCU is highly dependent on the provision of adequate resources for this effort, both at a system and a campus level. We will continue to identify information security as a high priority in resource planning and share the specific costs of providing security enhancements with the broader MnSCU community. We look forward to your continued advice and support as we move along an endless continuum of improving MnSCU information security.

Sincerely,

/s/ Ken Niemi

Ken Niemi
Associate Vice Chancellor for Information Technology & CIO
Minnesota State Colleges and Universities

EXECUTIVE SUMMARY

As of November 2000, the MnSCU wide area network consisted of 42,542 workstations connected to 725 servers, with countless miles of wire running through 941 wiring closets. Around 200,000 users have been granted access to MnSCU network resources; the rest of the world is able to reach some of these resources through the Internet. This framework serves as the foundation for MnSCU electronic communications and increasingly is becoming an essential component of the teaching and learning arena. Faculty store curricula and research on local area network servers. Student assignments are transmitted electronically. Even entire on-line courses are made possible by this technology.

Imagine if suddenly the MnSCU wide area network or one of the college or university local area networks was gone. What if an intruder stole valuable research materials or other sensitive data? The results could be traumatic. The risk of these problems is heightened without proper network security. In some respects, the network is only as secure as its weakest link. A weakness at one college or university may expose another one to security attacks.

The MnSCU Office of Internal Auditing conducted a system-wide study of network security. The study concentrated on network security issues presently under the control of each college and university. The study did not examine security issues related to the four MnSCU data centers. The Legislative Auditor has examined data center security in past audits. The study also did not consider security programmed into e-commerce applications that are in use. Although e-commerce security is important, MnSCU colleges and universities must first ensure that their networks provide a secure foundation from which e-commerce applications can operate.

The study confirmed that the threat of network security problems exists and is growing. Major corporations such as Microsoft and Amazon.com have been targeted by security attacks in the past year. Also, MnSCU colleges and universities have experienced about one security incident every other week. To date, MnSCU has avoided catastrophic results from a network security attack. It, however, has endured damages to websites, destroyed data files, and expensive damage from viruses. MnSCU data on students, research, and curricula are among the organization's most valuable assets. Inadequate network security exposes the organization to potential financial losses, denial of service, lost or corrupted data, unauthorized disclosure of confidential data, unauthorized use of resources, loss of public image or reputation, and the possibility of legal actions against MnSCU officials. Thus, it is essential that this information be protected from loss or damages.

The report offers recommendations for improvements to the Board of Trustees, System Office, and individual colleges and universities. It notes that increasingly organizations, including other higher education institutions are developing centralized information security policies. Therefore, it recommends that the board strengthen existing policy to address at least the following security matters:

- Establish an acceptable use policy,
- Define authorized users,
- Require password protection,
- Respect software licensing,
- Empower the system-wide security standards, and
- Require that security incidents be reported and tracked.

The report then recommends that the System Office translate board policy into procedures, standards, and guidelines to assist colleges and universities with network security matters. It recommends that the System Office develop or establish:

- Comprehensive procedures that outline minimum expectations for information technology security,

- Guidelines and standards to assist colleges and universities in developing campus specific policies and procedures,

- A process to guide the development, submission and review of college and university information technology plans, as required by board policy,

- Additional system-wide training opportunities, including development of a basic security awareness program targeted to users,

- A system to track and monitor security incidents that are reported by colleges and universities,

- A process to assist presidents with filling interim staffing needs when vacancies occur in critical IT positions at colleges or universities, and

- A strategy to coordinate implementation of firewall or similar technology throughout the wide area network. Only five of the sixty nine MnSCU local area networks are currently protected with firewall technology.

Finally, the report offers a series of recommendations to colleges and universities. It suggests that presidents review their organizational structures and staffing levels to ensure effective information technology services. Other recommendations address matters such as network infrastructure documentation, physical security, logical security, backup of data and program files, virus protection, and software licensing.

CHAPTER 1

THE THREAT IS REAL AND GROWING

MnSCU, like other organizations, is vulnerable to information technology (IT) security incidents. Colleges and universities rely on integrated systems for the majority of their administrative functions and increasingly for teaching and learning activities. Consequently, a security breach could result in significant financial losses, production time losses, damaged data integrity, or loss of research or other intellectual property.

MnSCU colleges and universities rely on technology for teaching and learning, as well as for the administration of the institution. This technology, in part, takes the form of integrated networks that are connected to the Internet. Faculty, staff and students rely on the availability of these networks as well as the accuracy of the data stored within them. The effect of losing network connections, even temporarily, could be devastating.

Local area networks (LANs) consist of workstations, laptops, servers, and other devices deployed in small geographic areas such as on a campus. Wide area networks (WANs) typically consist of two or more LANs connected across large geographic areas. The largest WAN in existence is the Internet. Exhibit 1-1 documents a simplified diagram of a LAN and definitions of common terms. Benefits to having LANs and WANs include: data management, information sharing, and the ability to share peripheral equipment (i.e. printers). The goal is to make all programs, equipment, and data available to anyone on the network without regard to the physical location of the resource, information or user.

Colleges and universities, like other organizations, are vulnerable to IT security incidents. A recent publication stated:

"...without adequate security protection, a network will be subject to complete disruption..."

> *Every institution has seen a rapid rise in the number of Internet-based security incidents and the losses in machine use, staff time, and data from those incidents. Ongoing attention to machine and network security is now necessary for the entire community of networked machines; without adequate security protection, a network will be subject to complete disruption at unpredictable and certainly inconvenient times.*[1]

Audit Scope, Objectives and Methodology

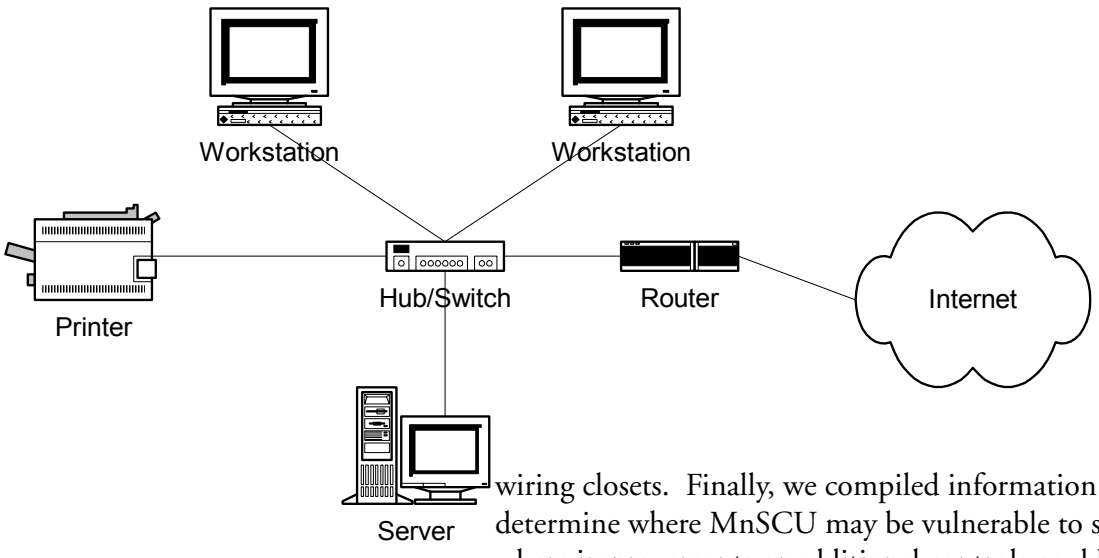
The primary purpose of this study was to gain an understanding of each MnSCU college and university network infrastructure and to review existing security policies and procedures.[2] Appendix A documents the objectives of this study as outlined in an audit proposal approved by the Board of Trustees on July 21, 1999.

We completed our review by interviewing IT staff at each college, university and the System Office. In addition, we completed walkthroughs at over 60 MnSCU sites to view physical security for servers and selected

[1] **Information Technology Systems, and Services in Higher Education: A Primer**, by Carole A. Barone, Robert F. German Jr., Richard N. Katz, Philip E. Long, and Barry Walsh; published by EDUCAUSE and NACUBO 2000.

[2] This study did not examine other important aspects of information security, such as controls over the four MnSCU data centers (the primary sites for processing and storing student and administrative data) or data security controls programmed into e-commerce applications.

Exhibit 1-1: Simple Local Area Network Diagram



wiring closets. Finally, we compiled information and evaluated results to determine where MnSCU may be vulnerable to security incidents and where improvements or additional controls could diminish exposure to vulnerabilities.

We verified select information obtained from the interviews, such as the existence of firewalls or access lists, but did not conduct detailed tests to verify all data reported to us. Although the study did not review system

Definitions of Common Network Terms:

- **Workstation** – single user computer like a personal computer. Typically, connected to form a local area network.
- **Server** – a computer or device on a LAN that manages network resources. For example, a file server is dedicated to storing files. Any user on the network can store files on the server. A print server manages one or more printers, and a

security at the four MnSCU data centers, the Legislative Auditor has reviewed it in past audits. For example, the Office of the Legislative Auditor released a report on November 22, 2000 that examined some aspects of security at the MnSCU data centers. The study also was not designed to address business continuity issues, such as loss of service due to natural disaster or accidents like disconnections due to severed telephone lines. MnSCU has, however, contracted with the Minnesota Department of Administration to assist it with developing a comprehensive business continuity plan.

This chapter provides some background on security vulnerabilities, recent incidents and impacts. In addition, the MnSCU IT infrastructure is summarized. The remaining chapters of this report focus on the results of our study. Chapter two discusses system-wide issues that could benefit from additional leadership and guidance from the Board of Trustees or System Office. Chapter three reviews network security elements under the primary control of individual colleges and universities. As part of our study, we developed a system-wide risk rating for select IT security measures (see Appendix B for a complete system-wide risk rating). Chapter three also examines the risk ratings in more detail and offers recommendations for colleges and universities to reduce vulnerabilities in key areas.

Information Technology Security Incidents

IT security threats are real. Former President Bill Clinton issued a Presidential Decision Directive in May 1998 calling for the federal government to produce a detailed plan to protect and defend America against cyber disruptions. Since that time, a number of significant IT related incidents have impacted large organizations in the United States. Exhibit 1-2 contains examples of these significant incidents.

What Could Happen?

A Trojan virus could result in unfettered access to the entire production system.

MnSCU could have been the victim in any of the examples listed in Exhibit 1-2. The denial of service attacks like the February 2000 incident show the potential for academic organizations like MnSCU to be used by hackers to launch the attacks. Also, consider the consequences if an attack similar to the Microsoft incident occurred at MnSCU. Because MnSCU relies on an integrated system, the installation of a Trojan virus on one of its workstations could result in unfettered access to the entire production system and all data. MnSCU is vulnerable to this risk because many colleges and universities do not keep virus protection software up-to-date on all workstations, laptops and servers. Without up-to-date virus protection software, MnSCU IT resources and data are at a greater risk of being impacted by Trojans or other viruses.

Also, an intruder potentially could alter, destroy, or steal confidential

accounting, human resource, student and academic (e.g., research, curricula, etc.) data. A recent legal memorandum[3] issued by the MnSCU General Counsel concluded that:

> *Litigation of privacy issues is increasing with the development of new laws and heightened public awareness. Claims against government entities and individuals for violations of data privacy interests may be brought under the Minnesota Government Data Practices Act and/or the Federal Educational Rights and Privacy Act. Additionally, individuals or entities may be liable under various tort or other statutory theories.*
>
> *In the event of civil litigation over alleged violations of data privacy interests, the State will defend and indemnify individuals who are found to be acting within the scope of their official duties and not with malice. Of course, any time these questions arise, legal counsel should be consulted.*

Exhibit 1-2: Examples of Recently Publicized Security Incidents

Date	Summary of Incident
October 2000	Microsoft Corporation disclosed that a hacker was able to break into Microsoft's internal network and access software source code that was in development. The cause was a form of a virus known as a Trojan that was installed on a workstation, allowing the hacker to penetrate their network.
May 2000	A computer virus known as the "love bug" impacted organizations worldwide. It is estimated that it impacted over 45 million personal computers and cost organizations over a billion dollars in software damage and lost commerce.
February 2000	Denial of service attacks *(an act intended to cause a service to become unavailable or unusable)* against Amazon.com, eBay, Yahoo and other e-commerce sites occurred. Estimates have put their losses at over $1 billion. In some cases, hackers had commandeered the IT resources of higher education institutions to launch these attacks. The institutions essentially enabled these attacks to happen due to inadequate security measures.

Source: Extracted from news accounts of the incidents.

[3] Legal Memorandum from Kristine Kaplan, Assistant General Counsel, to Ken Niemi, Associate Vice Chancellor MnSCU Information Systems, dated January 8, 2001.

Therefore it is essential that MnSCU officials demonstrate that they have taken reasonable and prudent precautions to protect information stored on and accessible through its networks.

What Has Happened?

A security incident is detected on average once every other week at a MnSCU college or university.

MnSCU colleges and universities have experienced many security incidents.[4] At a recent MnSCU Chief Information Officer (CIO) workshop, it was reported that a security incident is detected on average once every other week at a MnSCU college or university. Every incident requires staff resources to address it. Some attacks have resulted in unauthorized persons gaining control of MnSCU computers and using them to attack other sites on the Internet. Other attacks have been perpetrated by internal users. The following list provides selected examples of incidents that have occurred at MnSCU colleges and universities over the past year.

- √ A student loaded a virus into a technical college's network. The college estimated the incident cost $40,000 in employee time to isolate and remove the virus. In addition to the financial cost, there were public relations costs because media reported the incident on local television. The college expelled the student and turned information over to the Bureau of Criminal Affairs.

- √ An external organization notified a state university that it had been hacked into from a server from within the university. University employees determined that the server was in the College of Business and had not been sufficiently secured.

- √ A disgruntled employee, prior to leaving a community and technical college, deleted numerous files on a file server. It took college employees over 60 hours to find and restore all the deleted files.

- √ The MnSCU IT Services division noted that someone in Japan was using a community college web server inappropriately. Access to the web server was shut off.

- √ A local police department notified a technical college that someone had used a college color printer to produce counterfeit money.

- √ A hacker took over a state university web-site and posted "you have been hacked" on the site. Three more similar attacks occurred in

[4] Currently, there is no requirement for reporting and tracking security incidents (See Findings 1 and 2). The MnSCU ITS division estimates that it learns of only about one-half of the incidents that occur.

December 2000, possibly perpetrated by the same group. The Federal Bureau of Investigation is pursuing these cases.

These few examples show that incidents can be the result of external hacks and attacks. But they also show that not all threats are external to an organization. In many cases, internal exposures exist. Experts believe that internal threats are still the largest exposure to an organization's IT systems.

The Effect

MnSCU, like many other organizations, has endured security incidents. Whether malicious or not, these threats and exposures can and have resulted in:

- **Financial losses**. Anytime a security breach is detected, it takes employee time to resolve the incident. For example, when a virus is found on a PC or network, the network administrator must take time to isolate and remove the virus. In some cases, replacement of computer hardware may be needed.

- **Denial of service**. Any type of potential threat may reduce the availability of network resources to authorized users. For example, hackers may try to flood a system with e-mail activity that results in insufficient resources being available for legitimate network users. The loss of production time for faculty, staff and students is costly.

- **Lost or corrupted data**. Integrity of data is important to any organization. Colleges and universities should be particularly aware of academic data that needs to be secured. For example, faculty curriculum, student assignments, and student grades may be maintained on networks.

Unauthorized disclosure of confidential data could expose MnSCU officials to legal actions.

- **Unauthorized disclosure of confidential data**. Possible consequences are violation of law and policy or compromising student or employee rights. For example, colleges and universities may maintain student financial aid data, including family income information, on their networks. Unauthorized disclosure of this type of information from the student financial aid system could be very damaging and, as discussed earlier, potentially expose MnSCU officials to legal actions.

- **Unauthorized use of institution resources**. Possible consequences include the introduction of viruses, copyright violations for unlicensed software, and potential legal issues for damage done outside of MnSCU. For example, hackers could use Internet connections to

penetrate a college server and use it for destructive purposes, such as launching a denial of service attack against a commercial site. This type of activity could result in potential lawsuits against MnSCU.

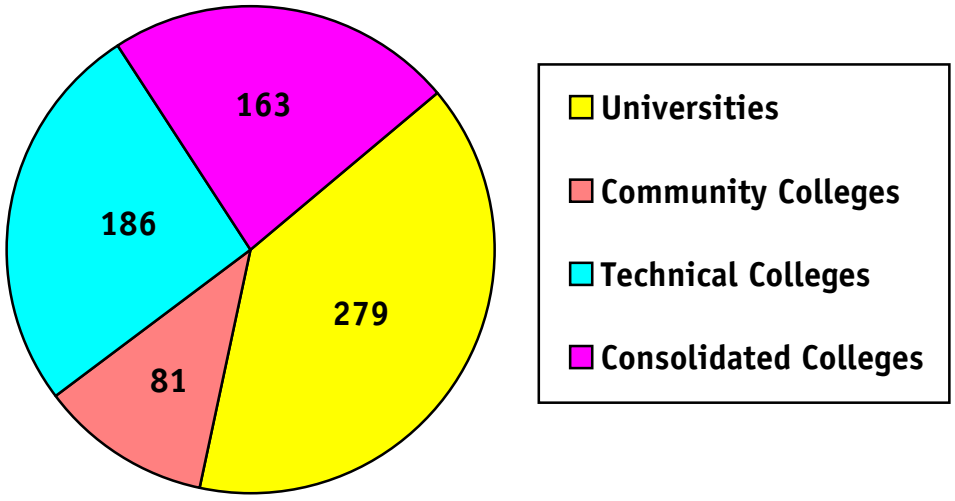
- **Loss of public image or reputation**. A valuable intangible asset worth preserving is an organization's image and reputation. Contributing to or being responsible for a breach of security could tarnish an organization's reputation.

MnSCU Information Technology Infrastructure

Today's technology requires integrated networks to be connected to the Internet. For example, MnSCU's centralized administrative systems are maintained at four regional data centers. Colleges and universities access these applications by connecting their local area networks to the MnSCU wide area network. In addition, more applications such as web registration and instructional technology software are being developed for access via the Internet. As a result, access to college and university data is no longer limited to a small geographic area.

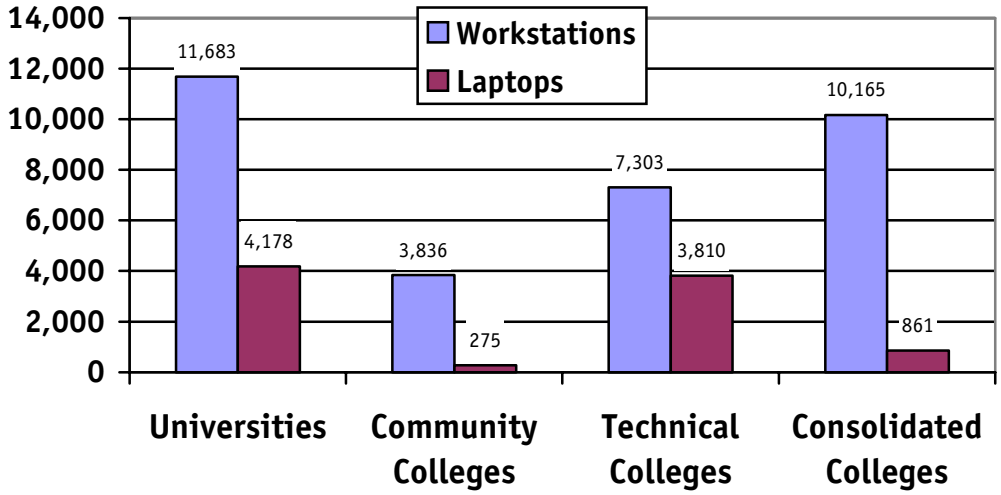
Each MnSCU college and university maintains at least one LAN at each of their campuses. Exhibits 1-3 and 1-4 document the number of servers, workstations and laptops maintained by MnSCU colleges and universities. Keep in mind that these numbers are constantly changing. MnSCU colleges and universities run a wide variety of operating systems on their LANs, including Novell NetWare, Unix, Linux and Microsoft Windows NT.

Exhibit 1-3: Number of Servers[1] at MnSCU[2] - November 2000



Note 1: About 17% of servers are outside jurisdiction of CIOs.
Note 2: The chart does not show the 16 servers maintained by the System Office.
Source: Interviews with college and university representatives.

Exhibit 1-4: Total Number of Workstations and Laptops at MnSCU[1] - November 2000



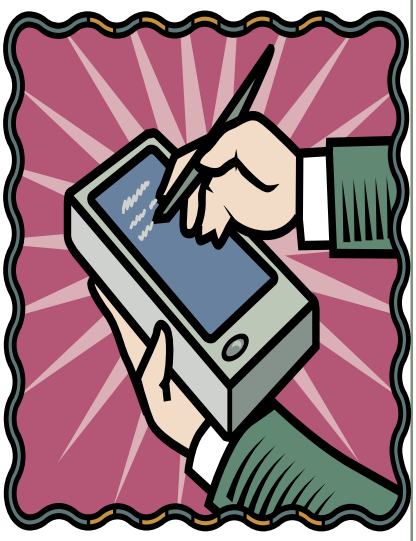
Note 1: The chart does not show the 331 workstations and 100 laptops owned by the System Office.
Source: Interviews with college and university representatives.

This page left blank intentionally.

CHAPTER 2

SYSTEM-WIDE SECURITY POLICIES AND GUIDANCE

The MnSCU Board of Trustees have enacted one general policy on information system security and approved an IT strategic plan submitted by the Chancellor. The board should consider incorporating additional features into extisting policy to set a tone about the importance of IT security and to clearly empower the Chancellor to direct security over matters that have system-wide implications.



The MnSCU System Office actively monitors the wide area network for possible security breaches. It also offers assistance on network security issues when requested by a college or university. To date, however, it has not established any system-wide procedures for system security nor offered appreciable guidance on security issues of common interest. Furthermore, the System Office has not made much progress on implementing the IT strategic plan or applicable provisions of board policy. Because the network security practices of individual colleeges and universities could imperil the security of the MnSCU wide area network or its data centers, it is essential for the System Office to assume a more active leadership role in this area.

Higher education, in general, has been known to have relatively open IT environments to facilitate the learning process. Due to recent incidents and concern over future vulnerability, however, the higher education community is being forced to review its practices and add controls to help manage the growing risk of security violations. Organizations such as EDUCAUSE[5] are helping the higher education community by highlighting potential risks and facilitating ways to build security foundations.

Several professional organizations have developed tools to help implement or revise IT security foundations. These tools focus on effectively controlling and managing IT. For example, the Information System Audit and Control Foundation named one such structure Control Objectives for Information and Related Technology (COBIT). This structure emphasizes 34 high-level control objectives that cover all aspects of information and the technology that supports it. A recent addition to the structure was a document that contains critical success factors, key goal indicators, and key performance indicators for each control objective.

Experts now suggest that a centralized security policy may be more effective.

Experts now suggest that a centralized security policy may be more effective than leaving the full responsibility to individual colleges and universities. For example, an article in the Information Systems Control Journal stated that "A centralized security policy provides organizations with much stronger control than a variety of policies that are haphazardly applied in different ways across different nodes and subnets of the overall corporate WAN and extranet"[6]

Our research of other higher education systems found that some governing boards are beginning to establish information system security policies. Exhibit 2-1 shows examples of some board policies on this subject. A task force of employees from colleges, universities and the System Office developed a MnSCU IT strategic plan that was formally approved by the Board of Trustees in January 2000. This strategic plan established an IT mission, as shown in Exhibit 2-2, and a governance structure. The plan does not specifically address the development of an IT security foundation. It does, however, create a system-wide technology roundtable that is empowered to recommend policy and engage in strategic planning. The System Office assembled the roundtable for its first meeting on January 26, 2001.

[5] EDUCAUSE is an organization whose mission is to help higher education institutions introduce, use, and manage IT. The organization recently initiated a security task force.

[6] Ayers, Susan and Fentress, Dave. "Enhancing IT Governance Through Enterprise Management Software Solutions." **Information Systems Control Journal** Volume 2 2000: 44+ .

Exhibit 2-1: Examples of Other Higher Education Information Technology Policies

System Name	Policy	Web-site Location
University of Minnesota	***Policy 2.8.1 Acceptable Use of Information Technology Resources.*** Most comprehensive policy and guidelines we found. It establishes an acceptable use policy, identifies authorized users, requires protection of passwords, and requires compliance with software licensing agreements.	www.fpd.finop.umn.edu/groups/ppd/documents/policy/Acceptable_Use.cfm
North Dakota University System	***North Dakota State Board of Higher Education Policy 1902.1 Computing Facilities.*** Policy addresses acceptable use of IT resources, requirements for protecting passwords, and compliance with software licensing agreements.	www.ndus.nodak.edu/policies_procedures/sbhe_policies/policy.asp?ref=2429
University of Wisconsin System	***Board of Regents Policy 97-2 Policy on Use of University Information Technology Resources.*** Policy addresses only acceptable uses of IT resources. It balances a free exchange of information against security considerations.	www.uwsa.edu/rpd/rpd97-2.htm
Montana Board of Regents of Higher Education	***Board of Regents Policy 1901.1 Unauthorized Copying and Use of Computer Software.*** Policy addresses only compliance with software licensing agreements.	www.montana.edu/wochelp/borpol/bor1900/1901-1.htm

Source: Higher education system web-sites.

Currently, MnSCU Board policy 5.13 contains the following policy related to IT security that was adopted in June 2000:

> *The chancellor shall develop an IT strategic plan for approval by the Board of Trustees and prescribe data, applications, security, and technology standards in order to ensure the effectiveness, efficiency, timeliness, and accuracy of information gathered, stored and utilized by the System Office, colleges, and universities. The chancellor shall review college and university IT plans.*
>
> *Each college and university shall adopt a campus policy on computer and network system use and security.*

Exhibit 2-2: The Mission of Information Technology Within the Minnesota State Colleges & Universities

We provide technological support for achieving success in the Minnesota State Colleges and Universities' learning enterprise. Our system and campus services:

- Enhance teaching and learning
- Support research, scholarship and creative activity
- Strengthen leadership, planning, and decision-making
- Support community building and community service
- Increase technology-user productivity
- Generate confident and satisfied students, faculty, and staff
- Ensure timely and efficient access to information

A key to our success is maintaining a balance between a reliable common infrastructure and the flexibility to tailor to local needs. Ultimately, we provide the innovative services and tools to help Minnesotans shape and adjust to the future in the Knowledge Age.

Source: MnSCU Strategic Plan and Proposed Governance Structure adopted by the MnSCU Board of Trustees in January 2000.

Some CIOs were unaware of existing board policy on IT security.

This policy has had little impact at the colleges and universities and we found that some CIOs were unaware of it.

MnSCU colleges and universities have been responsible for implementing their own security policies and procedures. However, with the reliance on integrated systems and the expanding role of the Internet, system-wide leadership is needed for IT security. As indicated in Exhibit 2-3, MnSCU colleges and universities struggle with having sufficient policies and procedures in place. In fact, many colleges and universities suggested that they would like to see system-wide policies and procedures to help guide them.

Having policies and procedures in place is essential for managing IT resources and data. These documents define expectations and requirements for managing IT security. In addition, these documents aid IT professionals in appropriately dealing with related incidents or requests.

Furthermore, it is difficult to hold employees and students accountable if expectations are not formalized or have not been clearly communicated. Therefore, it is important that network security responsibilities for users are clearly laid out in policies and procedures and communicated to faculty, staff and students.

Exhibit 2-3: College or University Level Network Security Policies in Place

Policy Name	Percent with Policies in Place.
Network Administration:	
• Network Security	16%
• System Backup	42%
• Virus Protection	21%
• Software Licensing	32%
• Incident Response	11%
• IT Strategic Plan/Work Plan	53%
User (faculty, staff and students):	
• Acceptable Use	68%
• Internet	61%
• Software Licensing/Copyright	50%

Source: Policies received from college and university representatives.

The MnSCU Board of Trustees must set the tone for information security.

As suggested by the MnSCU IT Strategic Plan, a key to success is balancing between common system interests and local needs. As discussed in finding 1, we believe that the MnSCU Board of Trustees must take the first step in setting the tone for information security interests and establishing a context for balancing system interests against local needs. Furthermore, as discussed in finding 2, we recommend that the MnSCU CIO work with colleges and universities to develop procedures for managing network security. In addition, we recommend that guidelines and standards be developed to help colleges and universities develop supplemental network security policies and procedures. Since a large percent of the colleges and universities do not have many policies and procedures in place, it makes sense to coordinate an effort to create them.

1. **The MnSCU Board of Trustees should consider incorporating additional features into existing policy to set a tone about the importance of IT security.**

Board Policy

Existing board policy delegates complete responsibility for network security matters to MnSCU colleges and universities. As discussed throughout this chapter, we believe there are compelling reasons for the board to establish a more comprehensive framework of expectations for IT security. Furthermore, a significant role should be reserved for the CIO, through the Chancellor, to establish procedures and guidelines to assist colleges and universities in securing their IT resources. Finally, a

reporting mechanism should be developed to assure the board that policy and Chancellor expectations are being fulfilled.

A recent report[7] on corporate governance identified some responsibilities for boards in helping set a priority over IT security. Some sample responsibilities included:

- Encouraging effective and responsible use of IT.

- Insisting that systems and their uses provide adequate management control and accountability balanced against the needs of the organization. Similarly, the board should require that information be protected from unauthorized or unintended modification, destruction, disclosure, or other endangerment.

- Asking questions of management to ensure that a sound information security program is in place.

As suggested in Exhibit 2-1, the governing boards of other higher education systems are beginning to address IT security concerns at a policy level. We recommend that the MnSCU Board of Trustees consider establishing a system-wide policy that includes, but may not be limited to, the following IT security matters:

- **Establish an Acceptable Use Policy.** Several colleges and universities had questions and concerns about their ability to impose any restrictions on the use of their network services. Some colleges and universities wondered if the concept of academic freedom disallowed them from placing any restrictions on use of the networks, particularly on Internet access. For example, is it possible for colleges and universities to disable Internet access to X-rated sites, an action taken by some other state agencies? There are several delicate legal considerations that affect matters such as the acceptable use of IT resources. A recent court case opinion ruled that higher education could restrict access to Internet data. The court ruled that a state regulation restricting access to data on the Internet did not infringe on a First Amendment right to academic freedom.[8]

[7] IIA [Institution of Internal Auditors], AICPA [American Institution of Certified Public Accountants], ISACA [Information Systems Audit and Control Association] and NACD [National Association of Corporate Directors]. Information Security Management and Assurance: A Call to Action for Corporate Governance. Altamonte Springs, Florida: IIA, 2000.

[8] Urofsky v. Gilmore, United States Court of Appeals for the Fourth Circuit. June 23, 2000.

- **Define Authorized users.** Policy should emphasize that those who access MnSCU networks must have some relationship to the college, university or System Office. Policy also could allow providing network services to certain users via contract, e.g., foundations. Access to MnSCU networks is not an unconditional right available to all citizens and organizations. Although it is sometimes not readily apparent, there is a cost to adding users to the network. As network traffic increases, eventually bandwidth must be expanded to support additional users. Also, colleges and universities may experience difficulty in enforcing acceptable use policies on users that are not accountable to them, e.g., community members. Some colleges and universities, however, believe that it is their responsibility to extend access privileges to members of the community, particularly through its library services. In other cases, colleges or universities continue to provide Internet services to former students and faculty members. A recent report captured the risk of these practices,

  > *In several extreme cases, colleges and universities find themselves serving in the role of Internet service provider (ISP) to the spouses and children of campus employees, emeriti, alumni, and others. In many of these cases, Internet access is provided at no cost, or at rates that are below campus costs. This situation is not only problematic financially but may be legally unsustainable, vis à vis commercial providers' concerns regarding predatory pricing by nonprofits.*[9]

Users should be subject to disciplinary action for failing to protect their password.

- **Require Password Protection.** Because networks may allow users to access information from virtually any location, network administrators rely on techniques such as User IDs and passwords to authenticate users' access rights to system data and resources. The effectiveness of these techniques is dependent on the willingness of users to protect the secrecy of their personal passwords. The obligation of users to protect their passwords is such a critical responsibility that it deserves emphasis in board policy. Furthermore, the policy should establish that users are subject to appropriate disciplinary action for sharing or neglecting to protect their passwords.

- **Respect Software Licensing.** Software licensing agreements typically restrict the use and distribution of the product. Although users may have access to these software programs for legitimate business uses, most licensing agreements would prohibit users from making copies

[9] **Information Technology, Systems, and Services in Higher Education: A Primer**, by Carole A. Barone, Robert F. German Jr., Richard N. Katz, Philip E. Long, and Barry Walsh; published by Educause and NACUBO 2000.

for personal use. Also, colleges and universities must have purchased enough copies to cover all users. If management fails to enforce these licensing agreements appropriately, it may face personal liability in the event widespread misuse of the product is discovered. Therefore, it is important for the Board of Trustees to establish the expectation that software licensing provisions will be observed and enforced. Again, the policy should establish that disregard of the licensing provisions will be subject to disciplinary actions.

If management fails to enforce licensing agreements, it may face personal liability.

- **Empower the System-wide Security Standards**. Board policy should also make it clear that the MnSCU Chief Information Officer, through the Chancellor's authority, is empowered to direct system security matters that have system-wide implications. Currently, MnSCU Policy 5.13 does empower the Chancellor to "prescribe standards" related to information security, among other matters. The authority of such standards is, however, unclear. This policy also states, "Each college and university shall adopt a campus policy on computer and network use and security." Board policy should be clarified to indicate that the colleges and universities are required to adhere to the Chancellor's security standards and should develop supplemental security policies specific to their unique situations. Furthermore, it should authorize the Chancellor to take emergency action to protect the wide area network (WAN) when warranted, such as disconnecting a local area network that places the WAN at risk. A final provision of existing policy requires the Chancellor to "review college and university IT plans." As discussed in Finding 2, however, there has not been much progress toward this requirement. Therefore, we recommend that the policy require a periodic monitoring report on progress toward completing these IT plans.

- **Require that Security Incidents be Reported and Tracked**. It is important that board policy require that security incidents be reported to the MnSCU Chief Information Officer. Another board policy in development proposes to enact this requirement. In October 2000, the board heard a first reading of MnSCU Policy 1.C.2 entitled, "Policy Against Fraudulent or Other Dishonest Acts". This new policy would require that "Dishonest acts that result in significant loss or damage to electronic information or information systems shall be reported to the MnSCU Chief Information Officer". A second reading and final board approval of this policy is expected in early 2001.

MnSCU executive management and the Board of Trustees are ultimately responsible for the organization and its assets. Therefore, these leaders need to set expectations for ensuring that IT resources are secure. A quote from a recent magazine article had an interesting implication;

Most exploits use known vulnerabilities – and most known vulnerabilities have known fixes, and they are free. The problem lies in organizations where security is not yet assigned a high priority.[10]

System-wide Recommendation

- *The MnSCU Board of Trustees should consider establishing a system-wide policy on several aspects of network security, including acceptable use, authorized users, password protection and software licensing. The policy should also empower system-wide security standards, require that security incidents be reported, and require periodic monitoring reports on progress toward implementing this policy. The board should obtain legal advice from the General Counsel so that the legal implications of network security are addressed appropriately.*

2. The MnSCU System Office has not exercised authority nor devoted sufficient resources to develop a solid foundation over IT security.

System Office Guidance

Over the past two years, the MnSCU Information Technology Services (ITS) division has been organized under the leadership of the MnSCU Chief Information Officer (CIO). As approved in the January 2000 IT Strategic Plan, the MnSCU CIO now reports directly to the Chancellor. The MnSCU ITS division currently includes approximately one hundred employees. In January 2000, the MnSCU CIO assigned responsibilities for coordinating system security to the former MnSCU Y2K Director. This director also has responsibilities for other major areas such as software development. The director currently manages about 35 employees; only one of these employees has responsibilities for system security issues. To date, the director and the one security employee have concentrated on issues regarding the MnSCU data centers and have not addressed college and university network security matters.

The MnSCU ITS division also has a four-employee group devoted to maintaining the MnSCU WAN. These employees have done a very effective job of monitoring the WAN for security violations. They also assist colleges and universities with troubleshooting network problems, handling incidents, and supporting networks. In addition, this group assists colleges and universities by monitoring security sites on the Internet and sending out e-mail messages to a MnSCU IT listserv to inform college and university CIOs of known vulnerabilities that should be fixed. This group is well-respected throughout the organization.

---

[10] Thibodeau, Patrick. "Experts Predict Rise In Severe Web Attacks." **Computerworld** 23 October 2000: 12.

The ITS division is planning to place a stronger emphasis on security.

The MnSCU ITS division has not taken steps to implement the provisions of MnSCU Policy 5.13.[11] It has not prescribed "data, applications, security, and technology standards in order to ensure the effectiveness, efficiency, timeliness, and accuracy of information gathered, stored and utilized by the System Office, colleges, and universities." Nor has it developed a process to "review college and university IT plans." According to the MnSCU CIO, the ITS division is planning to place a stronger emphasis on security and will devote more resources to build a security foundation if needed based on a risk assessment to be completed in the spring of 2001.

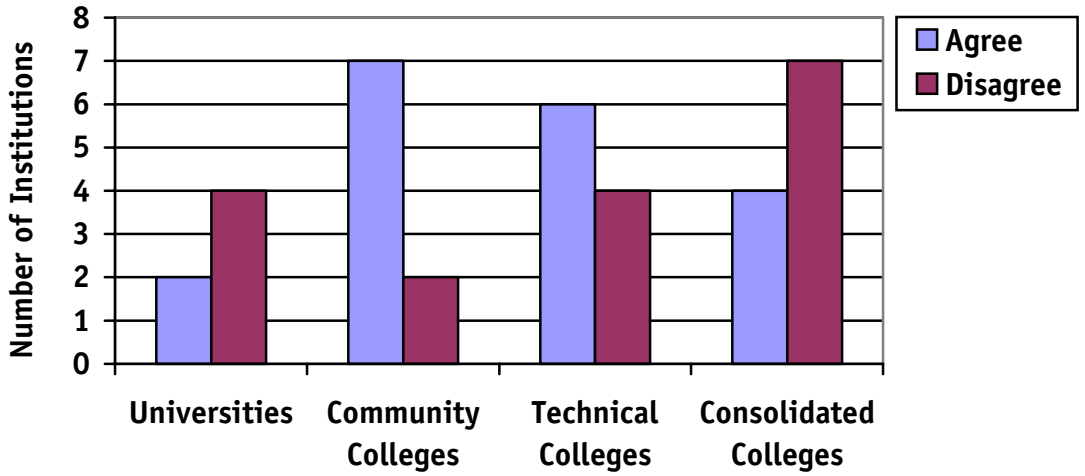
The MnSCU ITS division has attempted to help keep IT professionals current on relevant issues by sponsoring an annual training conference. This conference has been held the past two years and has included an IT security track. It has been well attended by MnSCU college and university employees. The ITS division has also hosted quarterly CIO meetings during the past year. In addition to providing IT training, these events have helped initiate networking opportunities for IT professionals within MnSCU.

As part of the study, we asked college and university CIOs to answer the following question: "Do you feel your IT function is adequately trained?" As you will see in Exhibit 2-4, the answers to the question fluctuated by institution type.

Many college and university CIOs commented that it would be helpful if the MnSCU ITS division would sponsor training on security and on specific IT topics. Those colleges and universities where adequate training seemed to be a concern noted the cost of technical training and felt it would be more cost beneficial if there were more internal training offered. It would also be helpful if the MnSCU ITS division developed a system to track and monitor security incidents (See Finding 1 regarding the need for a board policy to require incident reporting). Such a system would assist with identifying trends and patterns that could be incorporated into training programs or alerts sent to colleges and universities. The MnSCU ITS division could also assist colleges and universities by developing a basic awareness program that could orient users to their responsibilities (Also, see Finding 4).

[11] The policy technically assigns this responsibility to the Chancellor. Although we have not seen a formal delegation of this responsibility from the Chancellor to the MnSCU CIO and ITS division, we presume that they are the logical choice to carry out these duties.

Exhibit 2-4:
Is Information Technology Training Adequate?



Source: Opinions expressed by MnSCU college and university chief information officers.

Several colleges and universities reported difficulty filling vacant IT positions.

Finally, the employment market for hiring IT professionals is very competitive. Several colleges and universities reported difficulty filling vacant IT positions. Small colleges are at particular risk in this area, because they often rely on one key person to perform many essential IT responsibilities. The ITS division should consider the feasibility of coordinating efforts to assist presidents with temporary IT support for colleges or universities that suffer unexpected or sudden vacancies in critical IT positions (Also, see Finding 5). The MnSCU Finance division has recently implemented such a program to assist colleges and universities with transitions when critical finance-related positions become vacant.

System-wide Recommendations

- *The MnSCU Chief Information Officer should collaborate with colleges and universities to develop comprehensive procedures that outline minimum expectations for IT security for the approval by the Chancellor.*

- *The MnSCU Chief Information Officer should develop guidelines and standards to assist colleges and universities in developing campus specific policies and procedures.*

- *The MnSCU Chief Information Officer should develop a process to guide the development, submission and review of college and university IT plans; as required by MnSCU Board Policy 5.13.*

- *MnSCU ITS Division should analyze training needs of colleges and universi-*

ties to determine if additional system-wide training opportunities exist, including development of a basic security awareness program targeted to users.

- *MnSCU ITS Division should develop a system to track and monitor security incidents that are reported by colleges and universities.*

- *MnSCU ITS Division should assist presidents with filling interim staffing needs when vacancies occur in critical IT positions at colleges or universities.*

3. MnSCU needs to implement security technology to protect against threats through the Internet.

Firewall Technology

As indicated in Chapter 1, Internet based security incidents have been occurring at an alarming rate. One way to protect against these threats is to use firewall technology. A recent article states that:

> *A firewall is necessary for a network. Just as locks on a car or house keep unwanted people out, a firewall will help keep unwanted people out of a network. These measures are no guarantee of safety, but without them, you are making yourself a target for intruders.*[12]

Exhibit 2-5 shows by college and university type the technology in place, if any, to protect IT resources and data from external attacks. As the Exhibit shows, universities and community colleges are minimally protected.

Only five LANs are protected by firewall technology.

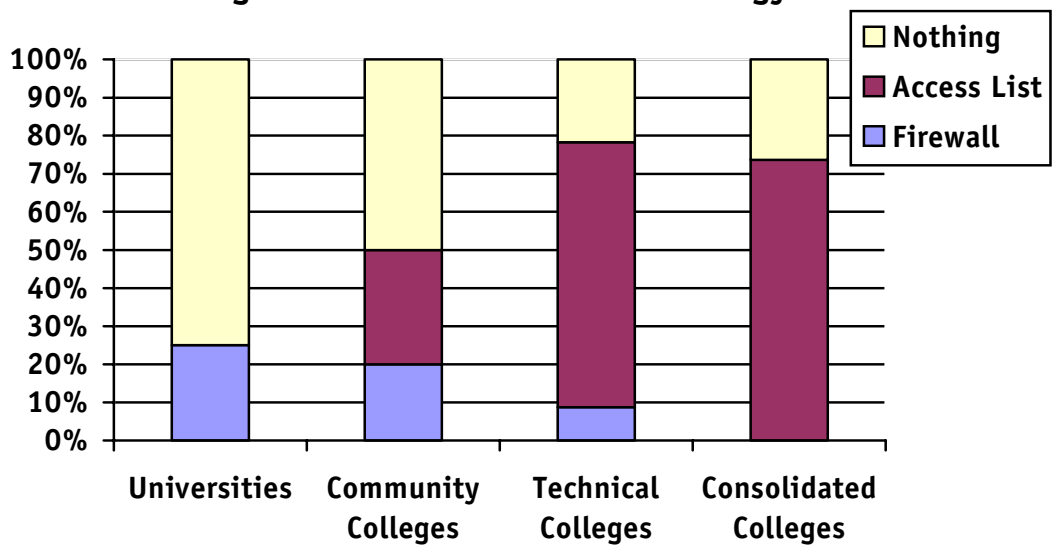
Only five of the local area networks connected to the MnSCU wide area network are protected from external attacks by firewall technology.[13] Consequently, most MnSCU colleges and universities are vulnerable to complex external attacks. This is alarming considering that security experts recommend having multiple firewalls in place. Most CIOs recognized the need for firewalls, but cited lack of funding as a reason for not implementing it. It is critical for MnSCU colleges and universities to implement firewall technology on all connections that have access to the Internet. Firewall technology, when managed effectively, will protect against external attacks via the Internet.

We did note that several MnSCU sites have implemented some technology

[12] Jones, Kyle. "Introduction to Firewalls." May 1, 1999. <http://www.itaudit.org/forum/network management/ftopnm.htp>

[13] This statistic does not include the four MnSCU data centers which are protected by firewall technology.

Exhibit 2-5: Protection against External Attacks
Percentage of MnSCU Sites with Technology in Place



Note: The chart does not show the two sites managed by the System Office.
Source: Information maintained by the MnSCU ITS division on 69 MnSCU sites.

to help protect the institution's network from external attacks. This technology is known as "access lists" or "packet filtering". This technology helps detect and prevent simple attacks and is a start at protecting networks. However, this technology is not sufficient to protect the college or university from complex attacks.

Because protection against external attacks is so critical to the preservation of MnSCU IT resources, we believe that the MnSCU ITS division must take the lead to coordinate the implementation of firewall or similar technology at all vulnerable points on the MnSCU WAN. This level of protection should be required as a condition for connecting a site to the MnSCU WAN.

System-wide Recommendation

- *MnSCU ITS should develop a strategy and coordinate implementation of firewall or similar technology throughout the MnSCU WAN.*

This page left blank intentionally.

CHAPTER 3

COLLEGE AND UNIVERSITY NETWORK SECURITY PRACTICES

Although the Board of Trustees and System Office can set expectations for protecting IT resources, it is ultimately up to colleges and universities to manage network security matters. Our interviews showed that many colleges and universities had made good progress to protect their networks, but additional controls are needed for nearly all the security measures that we evaluated.

As part of this study, Internal Auditing assessed the risk associated with 26 measures related to network security (see Appendix B). The results of these risk assessments were reported to college and university presidents and chief information officers as ideas to help them improve their operations. A summary of these risk assessments is presented throughout this chapter and related ideas for improvement are presented in Findings 6-14.

Leadership and human resources considerations are essential ingredients to managing network security effectively.

We also considered certain leadership and human resources factors that could affect network security at a college or university. Although not prone to ready measurement, leadership and human resources considerations are essential ingredients to managing network security effectively. Leadership factors such as the degree to which security policies and procedures are understood, the awareness of the importance of security measures, and the attitude toward vigorous implementation of policies and procedures set the stage for the security environment. Finding 4 suggests ideas for improving the awareness about security issues. The effective deployment of security measures is also dependent on human resources issues such as the background and experience of IT employees, lines of reporting, numbers of employees, and training and professional development practices. Finding 5 suggests security ideas related to human resources.

4. Colleges and universities must ensure that users of network services are aware of their responsibilities for protecting IT resources.

Many policies and procedures regarding network security are easily understood and make sense to IT professionals. However, IT professionals and management need to ensure that other individuals who use the IT resources understand the importance of the policies and procedures. For example, users need to understand why it is important not to share a password and what the consequences are if they do. A report, submitted to the Public Sector Chief Information Officers' Council by the Subcommittee on Information Protection in Canada in May 2000, cited the following:

> *Awareness and understanding is essential to implement information security policies and to ensure that related controls are working properly. Managers, users, and others with access to information resources cannot be expected to comply with policies they are unaware of or do not understand. Similarly, if they are not aware of the risks associated with their information resources they may not understand the need for and support compliance with policies designed to reduce risk.*[14]

[14] Canada. Treasury Board of Canada Secretariat. Chief Information Officer Branch. **Information Security: Raising Awareness, May 2000.**

A sound security foundation takes time to evolve. For that reason, it is critical to emphasize to faculty, staff, and students why complying with policies and procedures is important. Colleges and universities that do try to keep users informed of their responsibilities rely on a number of different approaches including:

√ Conducting one on one orientation with new faculty and staff.
√ Maintaining current policies and procedures on a web-site.
√ Requiring users to either sign a statement acknowledging their responsibilities or accept a statement when logging into the network.

College & University Recommendation

- *Colleges and universities need to be proactive in keeping faculty, staff and students informed of their responsibilities over IT resources and data.*

5. **Colleges and universities should examine their organizational structures and staffing levels to ensure that IT services are consistent with institutional plans and goals and are delivered in an effective manner.**

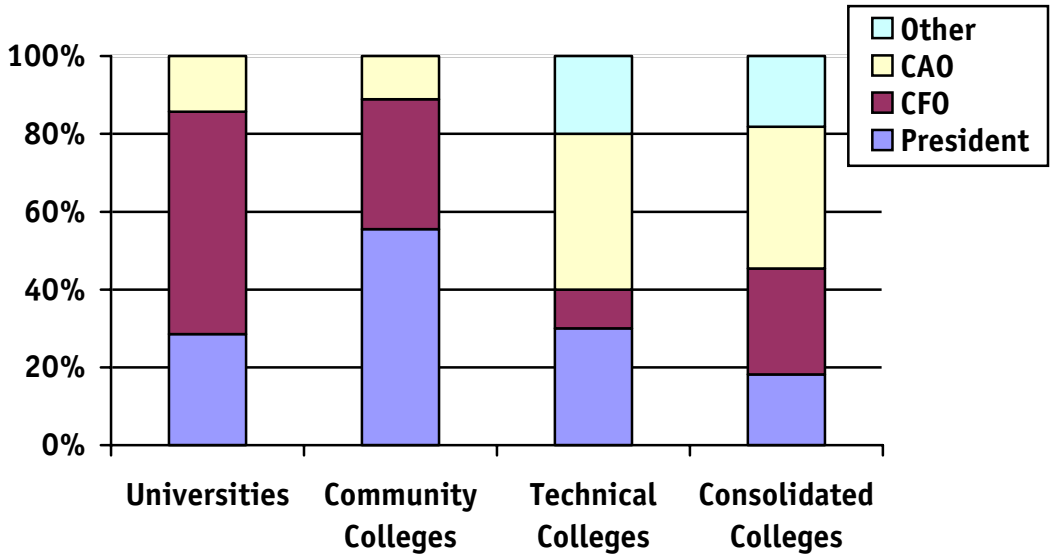
The complexity and reliance on IT today has prompted many organizations to place the administration of IT under one executive, often referred to as the chief information officer (CIO). The CIO position has grown in prominence over the last several years and this position is more frequently reporting to the chief executive of an organization.

Most of the MnSCU colleges and universities have organized the primary administration and security of IT resources and data under one individual. These individuals have many different titles and classifications, however, in this report we will refer to these employees as college and university CIOs. Exhibit 3-1 displays CIO reporting relationships at MnSCU colleges and universities.

Several incidents have occured from servers managed outside the IT area.

Several colleges and universities divided the responsibilities for managing IT. In some cases, separate sites or campuses were allowed to independently manage IT resources for that location. In other cases, the management of IT resources was different for administrative and academic employees. In most of these situations, the CIO did not have responsibilities for managing IT over the entire college or university. Of the total number of college and university servers, approximately 83% are managed by the CIOs. Under organizational structures where the CIO does not manage all IT resources, it is imperative to have minimum standards or guidelines in place for managing servers outside the primary IT area. Several incidents have occurred at MnSCU colleges and universities, from servers managed outside the IT area, because known vulnerabilities had not been fixed.

Exhibit 3-1: Chief Information Officers Lines of Reporting Percentages



Note: CAO = Chief Academic Officer
Note: CFO = Chief Financial Officer
Source: Interviews with college and university representatives.

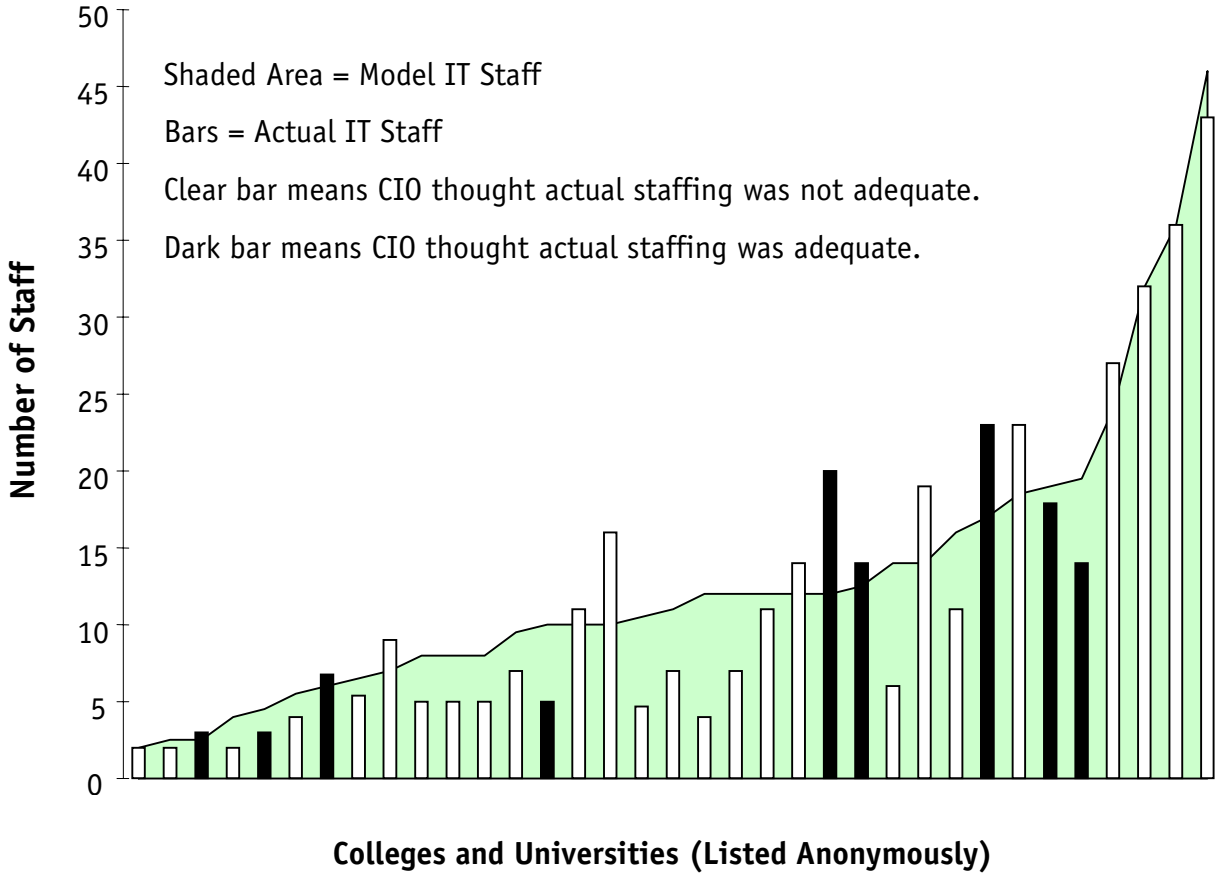
The study also found that several colleges are dependent on one key employee for managing IT. The reliance on one employee for managing all IT functions, including security, heightens the importance of having documented policies and procedures at a detailed level. If a key employee were to leave a college or univeristy or be unable to perform job responsibilities, the college or university would need to rely on its documentation in order to continue managing the IT function effectively.

Information Technology Staffing

As part of our review, we analyzed the size of IT staff groups across MnSCU colleges and universities. We compared current MnSCU staff sizes by different variables to estimate a model staff size. Exhibit 3-2 shows the variances noted between our calculated model staff size compared with actual size and the CIOs opinions of adequacy of staff size.

As Exhibit 3-2 shows, IT staffing varies significantly across MnSCU. Colleges and universities have many differences that need to be considered when determining an appropriate staff size for IT. We found that the following variables related to or impacted a college and universities staff size: number of workstations, number of laptops, number of sites, and number of full year equivalent students (FYE). However, there are other variables that impact staff size, but which could not be analyzed readily, including classification of positions, experience and knowledge of

Exhibit 3-2: Analysis of MnSCU IT Staff Sizes
November 2000



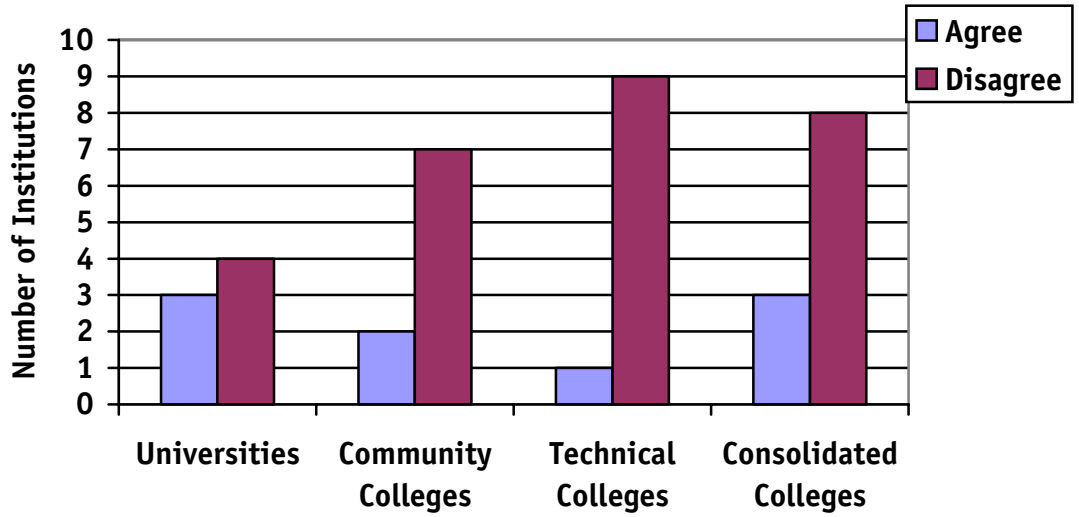
(1) Model IT staff sizes were projected using regression analysis based on data from MnSCU colleges and universities that reported the most secure network security environments. Independent variables used in the model were number of campuses, number of workstations, number of laptops, and Full Year Equivalent student counts.
(2) Each bar represents actual IT staff sizes reported by each MnSCU college or university. The data series is presented in order of the total number of computers (workstations and laptops) maintained by the college or university.
Source: Analysis prepared by the MnSCU Office of Internal Auditing.

staff, reliance on student workers, number of applications supported and the age and type of workstations. Also, responsibilities assigned to IT staff vary. For example, some IT staff also are responsible for maintaining audio visual equipment while others are not. Due to these other variables, it is difficult to judge what an ideal staff size should be. In addition, an IT consulting firm, the META Group[15], suggests that a driving factor in determining an optimal staff size is how well staff skills can be leveraged to fill the different roles that IT professionals are asked to perform. For

[15] The META Group helps companies make better IT decisions by providing research and unlimited analyst consultation relevant to their specific business needs.

example, IT employees are asked to wear many hats, including network support, help desk, project manager, report writer, system analyst, and educator to faculty regarding on-line methods for teaching and learning. As part of the study, we also asked college and university CIOs whether they felt their IT functions were adequately staffed. As you will see in Exhibit 3-3, most CIOs felt their IT functions were not adequately staffed. Several CIOs commented that this was a result of inadequate funding for IT or the difficulty of finding qualified candidates to fill positions.

Exhibit 3-3:
Is Information Technology Staffing Adequate?



Source: Opinions expressed by MnSCU college and university chief information officers.

College & University Recommendations

- *College and university presidents should analyze IT organizational structures to ensure that CIOs have adequate reporting relationships to produce effective network security functions and to ensure that service managed outside the CIO's jurisdiction are subject to adequate security measures.*

- *College and university presidents should review IT staffing with their CIOs to ensure that adequate resources are devoted to this important function. In some cases, presidents may want to consider alternatives in instances where a key employee resigns. Alternatives may include making arrangements with other MnSCU colleges or universities, the MnSCU ITS Division, or an outside vendor to provide interim services.*

Documentation

Overall, sufficient policies and procedures are not in place at many MnSCU colleges and universities and at the System Office for network security. In Chapter 2, we discussed the need for the Board of Trustees and the System Office to take the lead in setting policies and procedures for network security. Though ultimately, colleges and universities will have the responsibility for establishing effective practices for maintaining the security of their networks. It is essential that these practices be documented adequately to ensure that expectations are understood and that there will be a continuity of operations. As shown in Exhibit 3-4, network documentation must be improved at several colleges and universities.

Exhibit 3-4: MnSCU System Risk Rating
Network Infrastructure Documentation

Information Technology Risk Measures	System-wide Rating
Network administration policies and procedures (1) are in place.	
Detailed network diagram(s) exist.	
Policies and procedures (1) are in place & communicated to all users.	

Risk Level Legend: L - Low M - Medium H - High

(1) These measures examined whether colleges and universities had developed sufficient policies and procedures to compensate for the lack of system-wide policies and procedures.

Note: The system-wide rating is a composite of proportional risk ratings assigned to MnSCU colleges and Universities. Colleges and universities were asked to pay particular attention to those measures for which they were experiencing a High (red) risk of network security problems; these areas are subject to improvement. Measures evaluated as Medium (yellow) risk status were either in the process of becoming low (green) risk or the college or university has decided to accept the risk. (See Appendix B)

Source: Judgment of the MnSCU Office of Internal Auditing based on reviews of existing IT documentation and discussions with MnSCU colleges and universities and the System Office.

6. **IT documentation must be developed to ensure that network administrators and users (faculty, staff and students) know what they are responsible and accountable for.**

In addition to supplemental policies and procedures, colleges and universities must maintain an up-to-date and comprehensive network diagram. This diagram documents the location and connections of every piece of IT equipment. In addition, it documents information necessary for managing networks. For example, a diagram should contain the names

and purpose of all the servers within an organization. Without a diagram, IT professionals may have difficulty managing security over the entire technology environment. In addition, a documented network diagram will help smooth the transition when there is turnover in key IT positions or in recovery from a disaster.

College & University Recommendations

- *Colleges and universities should ensure that adequate policies and procedures are in place for IT security and related topics to supplement any MnSCU system-wide policies and procedures. Colleges and universities should also ensure that their policies and procedures are continually updated to reflect changes in business practices and technology.*

- *Colleges and universities should ensure that network diagrams are in place and updated regularly to reflect changes in network infrastructure. Copies of up-to-date network diagrams should be filed with the System Office as they are updated.*

Exhibit 3-5: MnSCU System Risk Rating
Physical Security

Information Technology Risk Measures	System-wide Rating
Physical access to the servers is limited (1).	
Physical access to wiring closets is limited.	
Physical access to hubs, switches, and routers is limited.	
Laptops not in use are stored in a secured location.	

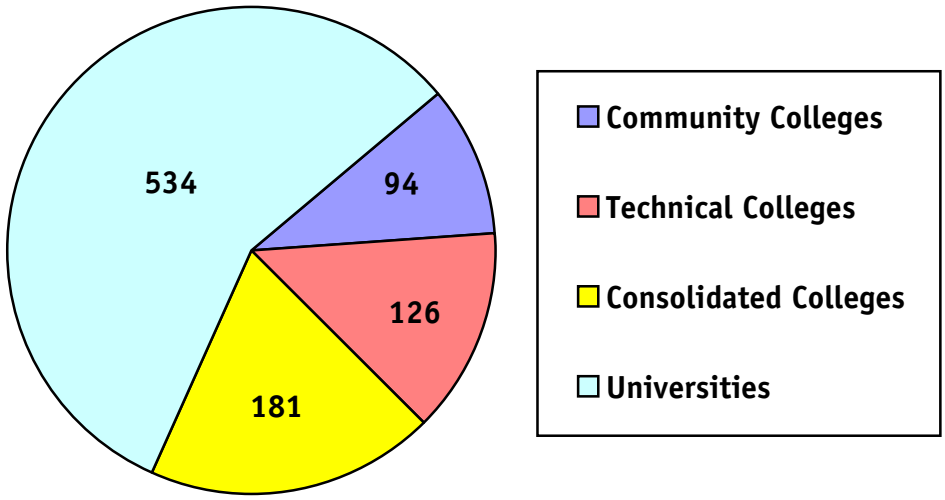
Risk Level Legend: L - Low M - Medium H - High

(1) The rating relates ONLY to servers under the administration of a CIO.
Note: See explanation of the system-wide risk rating on Exhibit 3-4.
Source: Judgment of the MnSCU Office of Internal Auditing based on reviews of existing IT documentation and discussions with MnSCU colleges and universities and the System Office.

Physical Security

Colleges and universities need to ensure that physical access to valuable IT equipment is limited only to individuals based on job responsibilities. As shown in Exhibit 3-5, the physical security of IT equipment needs improvement at most colleges and universities. The IT hardware infrastructure includes various pieces of equipment, including: servers, workstations, laptops, printers, and scanners. Typically, wire connects the equipment to build a network. The wire may run from an employee office or campus lab to a wiring closet. Devices such as switches, hubs and routers connect wiring closets to servers and the Internet.

Exhibit 3-6: Number of Wiring Closets at MnSCU



Note: The chart does not show the six wiring closets at the System Office.
Source: Interviews with college and university representatives.

Depending on the size, most colleges and universities have a minimum of one wiring closet for each floor of each building. Exhibit 3-6 demonstrates the number of wiring closets supported at MnSCU colleges and universities. As discussed in Chapter 1, colleges and universities also support numerous servers, workstations, and laptops. If this equipment were to become damaged or compromised it could result in significant consequences for the college or university.

7. **Physical security should limit access to IT equipment.**

Access to IT network equipment should be limited to the least number of individuals possible. Physical access should be restricted to individuals who maintain the equipment or whose other job responsibilities require it. In some cases, limited access to facility staff may be required for safety reasons. Limiting access to IT equipment protects it against damage from accidents and sabotage.

Our study noted several concerns with the physical access to IT equipment at colleges and universities.

- **IT equipment is located in public places.** Approximately half of the colleges and universities had some equipment located in classrooms, hallways or other public areas. Some campuses had wiring closets located in an area that anyone could access. In another case, a hub was located in a public hallway underneath a bench. In most of these

instances, IT staff were clearly aware of the vulnerability the location created. However, they lacked resources to rewire and move the equipment. Some colleges and universities are using lower cost alternatives to rewiring to help mitigate this risk. For example, some colleges had hubs located in public areas. Rather than relocating the hubs, it was often secured in a locked cabinet, a more cost effective option.

- **Access to equipment is permitted using campus master key.** Most colleges and universities have restricted access to the majority of IT equipment by locking the equipment in separate rooms. However, many of these same colleges and universities allow access to these rooms using campus master keys. In many cases, IT staff could not tell us who had copies of the campus master keys. In a few cases, master keys were given to all employees. Access to IT equipment should be granted to only those individuals whose job responsibilities require the access. Several colleges and universities have found alternatives for accessing server rooms and wiring closets. For example, one college has an IT master key that is distributed to only IT staff. Another college has installed a key card system to limit and monitor access to IT equipment.

- **Custodial staff had access to server rooms and wiring closets.** Over 80 percent of MnSCU colleges and universities allow custodial staff access to server rooms and wiring closets. In many cases, wiring closets are located within the custodial closets. This is more prominent in older buildings where wiring was installed after buildings were built. In a physical walkthrough of one college, we viewed cleaning products and ladders leaning against IT wiring. CIOs again recognized these vulnerabilities and told us that as buildings are remodeled these conditions are remedied. A few colleges and universities with this scenario have placed the IT equipment in locked cabinets to help protect it. Industry best practices recommend that custodial staff be restricted from areas where IT equipment is located and recommend IT staff accompany custodial staff when these areas are being cleaned.

With the evolution of IT uses in teaching and learning, many colleges and universities have started programs that require students to have laptop computers. Also, many colleges and universities either provide laptops to employees or have a system for checking out laptops to employees when needed. Laptop computers are known to be vulnerable to theft and therefore need to be adequately safeguarded.

All colleges and universities and the System Office maintain some laptop computers for faculty and staff use. In addition, a few campuses maintain large laptop computer inventories to issue to students. It is imperative that the laptop computers are adequately secured when not in use. Several

colleges and universities and the System Office have reported thefts of laptop computers in the past year. It is critical to encourage staff to adequately protect laptop computers. Colleges and universities should consider establishing physical security guidelines for laptop computer users. Some suggested methods for protecting laptop computers include: password protecting, locking laptops in offices or cabinets when not in use, locking laptops to desktops, and using laptop case alarms.

College & University Recommendations

- *Colleges and universities should limit physical access to IT equipment to only those individuals with job responsibilities requiring access.*

- *Colleges and universities should establish guidelines regarding security for laptop computers used by students and employees.*

8. IT equipment should be located in environmentally sound locations.

IT equipment, as well as the software and data maintained within the equipment, are important assets to colleges and universities. IT equipment is sensitive to its environmental surroundings and cannot, for example, be located in an area with extreme heat. We noted several environmental issues at colleges and universities over the primary IT equipment, including IT equipment located:

- In a room that had no fire protection.
- In a room where the roof leaks.
- In the same room where the boilers for the campus are located.
- In a room without temperature and humidity controls.

These concerns need to be addressed in order to prevent network failure due to the physical location of the equipment.

College & University Recommendation

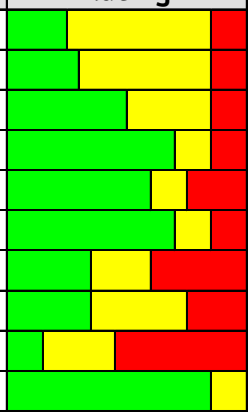
- *Colleges and universities should consider environmental factors, such as temperature, humidity, and sprinkler system, when determining the location of IT equipment.*

Logical Security

Most colleges and universities have implemented logical security controls on local area networks to limit access to resources and data. However, as discussed in Chapter 2, MnSCU is vulnerable to threats through the Internet since only five colleges and universities have implemented firewalls. Exhibit 3-7 shows the system-wide risk rating for specific logical security measures evaluated

Exhibit 3-7: MnSCU System Risk Rating
Logical Security

Information Technology Risk Measures (1)	System-wide Rating
Process in place for adding users to network.	
Process in place for changing or removing user access.	
Authorized user lists are reviewed periodically.	
Administrator rights are limited.	
Administrators use separate account for daily activities.	
Password security used on servers connected to WAN.	
Users are required to change passwords periodically.	
Shared accounts are not used.	
Technology in place to manage remote access via Internet & dial-up.	
Servers are not being used as workstations.	



Risk Level Legend: **L** - Low **M** - Medium **H** - High

Please note - We did not complete detailed testing on these areas.
(1) The ratings relate ONLY to servers under the administration of a CIO.
Note: See explanation of the system-wide risk rating on Exhibit 3-4.
Source: Judgment of the MnSCU Office of Internal Auditing based on reviews of existing IT documentation and discussions with MnSCU colleges and universities and the System Office.

at MnSCU colleges and universities and the System Office.

Logical security is as basic as requiring a login ID and password to get into a computer or as complex as building multiple firewalls (see Finding 3 for a discussion about firewalls) to protect organizations from intruders. Without the use of different layers of logical security, an organization would be subject to unlimited vulnerabilities.

9. Colleges and universities need to improve the management of accounts on local area networks.

It is common industry practice to establish user accounts to obtain access to IT resources and data, and this is true at MnSCU colleges and universities too. Faculty, staff and students use login IDs and passwords to use network resources and access data. Using login IDs and passwords is a method for authenticating users by confirming who is trying to use the resource, limiting access to resources and data, and protecting individuals. We noted the following concerns related to accounts on local area networks:

- **Allowing external parties access to IT resources.** MnSCU colleges and universities take an active role in the communities that surround

them. Consequently, many colleges and universities provide various organizations with access to network resources. These relationships may expose the college or university to additional vulnerabilities, as well as take up scarce resources. Although many of these relationships serve an appropriate purpose, colleges and universities need to take a close look at the relationships to make sure that they are within their mission. In addition, management needs to define who are the members of the campus community and to what resources they are entitled. Furthermore, colleges and universities should have contracts with any outside organizations.

- **Insufficient process for adding users to the network.** Colleges and universities need to ensure user access is limited to need. By not having a written process in place for authorizing access to IT resources, network administrators have difficulty challenging the appropriateness of specific access requests and may grant access to inappropriate users.

- **Insufficient process for changing and removing user rights.** Colleges and universities should ensure that only authorized users have access to IT resources and data. A written process needs to be in place that notifies system administrators when an employee's position changes or when a user leaves the college or university.

- **Insufficient process for validating the authority of users.** Colleges and universities should periodically review authorized user lists to ensure that only authorized users have access to the network.

- **Not requiring users to change passwords periodically.** Implementing periodic password changes is an important control to help protect systems from unauthorized access. The use of passwords authenticates the identity of a user to a specific person. Individuals may compromise their password for a variety of reasons. Enforcing periodic password changes minimizes this risk.

- **Not requiring unique accounts (login IDs) and passwords for all users.** The use of unique accounts and passwords by all individuals is an important control to ensure accountability. When individuals share accounts, it becomes nearly impossible to trace actions to a specific user. It is particularly risky when individuals with capability to update the network share accounts and passwords.

  Several colleges and universities did not require individuals to have unique accounts where "view only" access was allowed in community areas, such as computer labs or libraries. Allowing individuals the ability to use network resources without identifying them precludes

holding them accountable for their actions. Colleges and universities need to fully and reasonably manage these risks. The following list contains possible alternatives for minimizing this risk:

- Limiting access to specific applications (locking down workstations to prohibit users from changing the configuration).
- Restricting accounts to specific workstations.
- Imposing time restrictions on these accounts.
- Requiring individuals to sign a log when using workstations.
- Programming workstations to reset them to the original configuration upon rebooting.

We also found that a few colleges and universities did not require unique accounts for all individuals with update access to network resources. All individuals that have capability to update any network resource should have a unique account to ensure individual accountability for actions performed on the network. For example, all student workers should have unique accounts.

- **Not limiting the number of unsuccessful login attempts into the network.** Computerized tools exist that permit individuals to guess passwords. One way to minimize the risk of these individuals guessing passwords is to limit the number of unsuccessful login attempts into the network. This is particularly important when the college or university allows remote access into the college or university's network.

College & University Recommendation

- *Colleges and universities need to ensure that appropriate controls are in place on network accounts.*

10. Colleges and universities need to improve controls over powerful accounts on local area networks.

Network administrators need an account with powerful access (administrator rights) to administer and manage local area networks. This access gives administrators complete and unfettered access to data and software programs. As Exhibit 3-7 illustrates, most colleges and universities have effective controls in place for individuals with administrative rights. However, we did note certain weaknesses regarding these powerful accounts, including:

- **Not limiting administrative right access.** Granting users more access than needed to complete their job responsibilities creates an unnecessary security risk. To improve controls, colleges and universities should define security clearances for individuals that are appropriate for their specific job duties.

- **Not using separate accounts for daily activities.** Several colleges and universities had network administrators who did not use a separate account to complete daily activities, such as using word processing or e-mail applications. Network administrators that use accounts with administrator rights to complete daily work, particularly when using the Internet, expose the college or university to unnecessary risk. Computerized tools exist that permit individuals to obtain account information and passwords when these accounts are open for long periods to conduct routine, daily work. The unauthorized use of accounts with administrator rights exposes the entire organization to significant and unnecessary risks. The use of separate accounts by network administrators, when completing daily activities, reduces the risk of unauthorized access to the network.

College & University Recommendations

- *The use of powerful accounts should be limited to only individuals whose job responsibilities require the access.*

- *Individuals with powerful accounts should use a separate account for routine, daily activities.*

11. Colleges and universities need to ensure that sufficient controls are in place over remote access to network resources.

It is becoming increasingly important for network administrators to provide students, faculty and staff with remote access to network resources. This access is gained through software used for dial-up or directly over the Internet. We noted that two-thirds of MnSCU colleges and universities provide some form of remote access to faculty, staff and/or students. However, permitting this access to the network provides hackers opportunities to gain access to campus resources and data. There are many different software programs available that allow remote users into a network.

Experts recommend that at least two forms of authentication be used when providing remote access to users. We caution colleges and universities to verify that appropriate security measures are in place to ensure that only authorized users gain access to network resources.

College & University Recommendation

- *Colleges and universities need to ensure that controls are in place over remote access to network resources and data.*

Virus Protection

MnSCU colleges and universities understand the importance of having anti-virus software programs on workstations and servers. However, several colleges and universities still need to install anti-virus protection on selected workstations and servers. In addition, some colleges and universities need to improve processes for updating anti-virus software programs.

Exhibit 3-8 shows the system-wide risk rating for specific virus protection measures evaluated at MnSCU colleges and universities and the System Office.

Exhibit 3-8: MnSCU System Risk Rating
Virus Protection

Information Technology Risk Measures (1)	System-wide Rating
Virus protection is on all workstations and laptops.	
Virus protection is on all servers.	
Virus protection signatures are updated, as they become available.	
Updates to virus protection software signatures are automated.	

Risk Level Legend: L - Low M - Medium H - High

Please note - We did not complete detailed testing on these areas.
(1) The ratings relate ONLY to servers under the administration of a CIO.
Note: See explanation of the system-wide risk rating on Exhibit 3-4.
Source: Judgment of the MnSCU Office of Internal Auditing based on reviews of existing IT documentation and discussions with MnSCU colleges and universities and the System Office.

In Chapter 1, we discussed the vulnerabilities that MnSCU could have to a recent incident occurring at Microsoft Corporation. According to news accounts, the virus that penetrated Microsoft was not new and should have been detected by anti-virus software. However, it wasn't. The attack was likely successful because someone disabled the anti-virus software, or a workstation did not have the most recent anti-virus software update installed. A November 1, 2000 article report the incident this way:

> *The moral here is obvious, and could become incredibly expensive if you fail to take heed. Be certain you have antivirus software in place, at least at the desktop level. Never turn the software off unless you absolutely have to (and then only for brief instances under strict policy), and regularly check (perhaps daily, again under strict policy) to ensure*

you have the latest antivirus signature files installed on your systems.[16]

12. MnSCU needs to ensure that adequate protection is in place to protect networks from computer viruses.

All workstations, laptops, and servers need to have adequate virus protection software programs installed to help safeguard software, hardware, and data from damage. As Exhibit 3-8 shows, most colleges and universities have virus protection software installed on workstations and laptops. It also shows that about half the colleges and universities have virus protection software installed on all servers. Below are concerns that indicate MnSCU colleges and universities may be vulnerable to computer viruses.

- 19 colleges and universities have not installed virus protection software programs on all laptops, workstations, and servers. To reduce vulnerability, colleges and universities need to install virus protection on all platforms.

- Virus protection software updates were not performed regularly on all laptops, workstations, and servers. Virus protection software is only as good as the last update. In order to ensure protection from known viruses, the virus definition files and the scanning engine must be updated timely.

- Several colleges and universities left the primary responsibility for applying updates to the virus protection software to individual students, faculty, and staff. To ensure that the network is adequately protected from viruses, updates to virus protection software should be automated or at least centrally administered to everyone.

- Several colleges and universities did not limit the ability to disable virus protection software. Colleges and universities should ensure that safeguards are put in place to prevent users from disabling virus protection software. An incident discussed in Chapter 1, at a MnSCU technical college, could have been prevented if the ability to disable virus protection had been limited. In some cases, there may be a legitimate reason for allowing users to disable software or limitations within the software itself. Whatever the reason, the institution needs to be aware of the additional risk and consequences that may occur if such protective software is disabled.

[16] Edwards, Mark Joseph. "Microsoft Break-in: A Lesson in Desktop Security." **Windows 2000 Magazine.** November 1, 2000 <http://www.win2000mag.net/email/index.cfm?ID=5.>

The System Office detects one or two viruses a day by scanning e-mail.

In addition, colleges and universities should consider adding additional controls to prevent or detect the spread of computer viruses. For example, an InterTechnologies Group[17] manager recommends that all incoming and outgoing e-mail messages be scanned for computer viruses. The InterTechnologies Group provides this service to most state agencies and would consider scanning MnSCU's e-mail for computer viruses, depending on the Group's capacity. Currently, the System Office provides this control internally which protects System Office employees from receiving or sending computer viruses to other Internet users. A System Office IT employee reported that they detect one or two viruses a day by scanning e-mail.

College & University Recommendations

- *Colleges and universities need to ensure that virus protection software is installed on all servers, workstations, and laptops and is updated on a timely basis.*
- *Colleges and universities should develop a process to automate the distribution of virus protection software updates.*
- *Colleges and universities should limit the ability to disable virus protection software.*
- *Colleges and universities should consider scanning e-mail messages for computer viruses.*

Backup

Most MnSCU colleges and universities complete backups of data and programs. However, many colleges and universities do not store backup tapes offsite and/or in a secure location. Exhibit 3-9 shows the system-wide risk ratings for specific backup measures evaluated at MnSCU colleges, universities, and the System Office.

13. Colleges and universities need to ensure that sufficient controls are in place for backing up data and programs.

Network failures or disasters such as fires or floods result in disruptions to normal operations. These disruptions can and do occur at inconvenient times. Having comprehensive backups of data and programs help to minimize the downtime due to these disruptions. Without adequate backup, recovery of data and programs is difficult, if not impossible.

[17] The InterTechnologies Group is a division of the Minnesota Department of Administration and is the core computer operations organization for State of Minnesota agencies, providing services for managing and operating IT resources.

Exhibit 3-9: MnSCU System Risk Rating Backup

Information Technology Risk Measures (1)	System-wide Rating
♦ **Backup**	
Backups of data and programs are performed daily.	
Backup tapes are stored offsite in a secure location.	
Periodic test-restores are completed on backups.	

Risk Level Legend: **L - Low** **M - Medium** **H - High**

Please note - We did not complete detailed testing on these areas.
(1) The ratings relate ONLY to servers under the administration of a CIO.
Note: See explanation of the system-wide risk rating on Exhibit 3-4.
Source: Judgment of the MnSCU Office of Internal Auditing based on reviews of existing IT documentation and discussions with MnSCU colleges and universities and the System Office.

As Exhibit 3-9 illustrates, most colleges and universities completed daily backups of data and programs, but did not store backup tapes offsite in a secure location. We found most colleges and universities have copies of backup tapes taken offsite weekly. However, these backup tapes are not always stored in environmentally secure locations. In many cases, we found that network administrators were taking the backup tapes home. It is notable that these network administrators appreciated the importance of maintaining backup tapes off-site, nevertheless, their homes are not the best storage location.

In an ideal situation, a courier service should pick up backup tapes on a routine basis and take them to a secured storage facility. These facilities are designed to provide protection to backup tapes from unauthorized access and environment factors such as extreme heat or humidity. While this type of service may not be available in all parts of the state, some colleges and universities have come up with alternatives. For example, some multi-campus colleges and universities swap backup tapes between campuses. In other cases, colleges and universities have looked to other state agencies to provide secure storage.

Another important feature to backup of data and programs is periodic testing to verify that data and programs stored on backup tapes can be restored to a server or workstation. If employees do not test this capability and maintain the ability to quickly reinstall data and programs, efforts to restore data and programs at the time of a disruption may be more time consuming or even futile.

College and University Recommendations

- *Data and programs should be backed up on a daily basis.*
- *Backup tapes should be stored off-site in an environmentally secure location.*
- *IT staff should regularly test to verify that data and programs on backup tapes can be restored quickly and accurately.*

Software Licensing Compliance

MnSCU colleges and universities, for the most part, could make improvements to the process of complying with software licensing agreements. A good starting point is to keep a complete up-to-date inventory of all software programs. Exhibit 3-10 shows the results of our system-wide risk assessment for software licensing. Software management is an important business practice. The benefits of software management include ensuring legal compliance with licensing agreements, controlling costs associated with software purchases and improving software assets contribution to organizational performance.

Exhibit 3-10: MnSCU System Risk Rating
Software Licensing

Information Technology Risk Measures (1)	System-wide Rating
♦ **Software Licensing**	
A software inventory is maintained and updated regularly.	
A process is in place for complying with licensing agreements.	

Risk Level Legend: L - Low M - Medium H - High

Please note - We did not complete detailed testing on these areas.
(1) The ratings relate ONLY to servers under the administration of a CIO.
Note: See explanation of the system-wide risk rating on Exhibit 3-4.
Source: Judgment of the MnSCU Office of Internal Auditing based on reviews of existing IT documentation and discussions with MnSCU colleges and universities and the System Office.

Software piracy can expose colleges and universities to both civil and criminal liability, in addition, colleges and universities could experience tarnished reputations for being found liable for copyright infringement. Exhibit 3-11 lists examples of software piracy. While many people may believe there is little chance of being caught, they are wrong. According to the Business Software Alliance (BSA) 1997 statistics, "on average at least one company is caught and confronted with the threat of legal proceedings every

working day."[18] The BSA is generally notified of copyright infringement by calls from employees or former employees on its anti-piracy hotlines.

Exhibit 3-11: Examples of Software Piracy

Purchasing one licensed copy of a software program and installing it on multiple computers.
Downloading software from the Internet (other than freeware).
Taking advantage of upgrade offers without having a legal copy of the version being upgraded.
Swapping disks or CDs within or outside the workplace.
Purchasing illegally duplicated copyrighted material.
Exceeding the permitted number of users for a software program loaded on a network server.

Source: Prepared by the MnSCU Office of Internal Auditing.

As discussed in Chapter 2, having policies and procedures in place is essential for managing IT resources and data. As earlier noted in Exhibit 2-3, only 32% of MnSCU colleges and universities have a network administration software licensing policy in place and 50% of MnSCU colleges and universities have a software licensing policy in place covering users. This is an alarming statistic, since a recent poll of other higher education institutions found that over 85 percent had a policy in place or in development.[19]

14. MnSCU needs to have a process in place for complying with software licensing agreements.

Colleges and universities use numerous software programs within academic programs and to help with administrative and management functions. Campus leaders need to be aware of requirements of software licensing agreements and the risk that noncompliance brings. Many colleges and universities feel they have found some protection by entering into software agreements with vendors, such as the Microsoft agreement. These agreements may help in ensuring compliance with a specific application or set of applications, however, the institution as a whole needs to determine how it plans to meet compliance with software licensing agreements.

An important part of complying with software licensing is having a process in place for taking corrective action when noncompliance is discovered. During the course of our study, IT staff from a few colleges and universities expressed concern over their lack of power to remove unauthorized software from workstations.

[18] The Business Software Alliance Guide to Software Management. <http://www.bsa.org.>
[19] EDUCAUSE, The Pocket Guide to U.S. Higher Education, October 2000

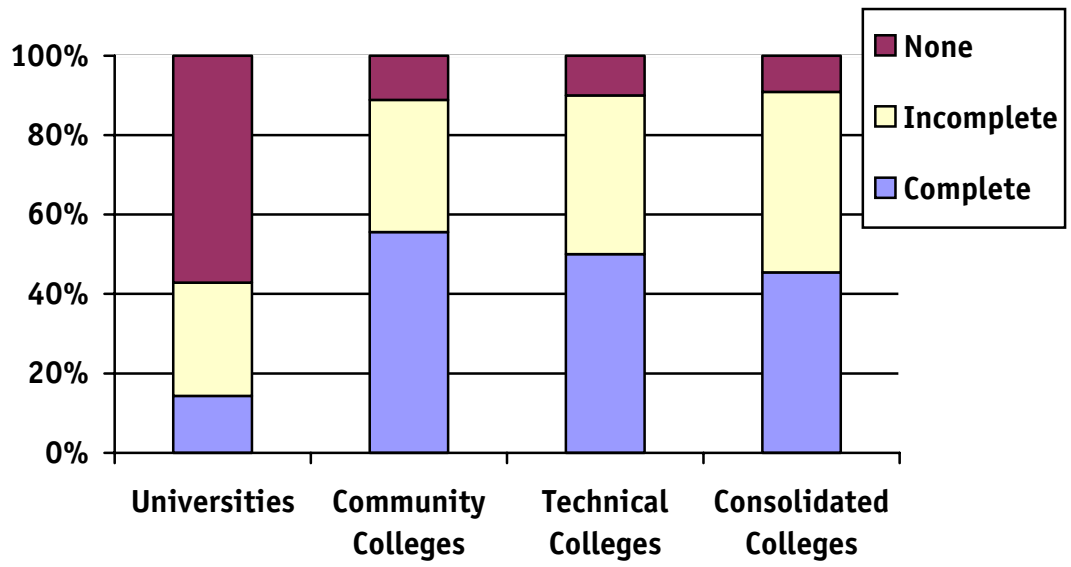
A good foundation for having an effective software management process is keeping a comprehensive up-to-date inventory of all software residing on workstations, laptops and servers. As noted in Exhibit 3-12, many MnSCU colleges and universities do not keep this type of inventory. Our study found, however, that colleges and universities with a comprehensive software inventory generally require software purchases to go through a centralized process. Without an inventory, colleges and universities may have difficulty proving what software licenses exist or how many software licenses are needed.

Another good practice in effective software management is to keep original licenses, documentation and original diskettes or CDs for all purchased software in a secure location.

College & University Recommendations

- *Colleges and universities should have a process in place to monitor compliance with software licensing agreements.*
- *Colleges and universities should have a process in place to manage issues that arise over software licensing. For example, IT staff should be allowed to remove unauthorized software from workstations.*
- *Colleges and universities should maintain an up-to-date inventory of all software.*

Exhibit 3-12: College and University Software Inventories



Source: Interviews with college and university representatives.

Appendix A

MnSCU Office of Internal Auditing
Audit Proposal

The MnSCU Board of Trustees Audit Committee reviewed the Internal Auditing proposal to study local area network security on July 21, 1999. The proposal cited the following objectives.

OBJECTIVES:

1. Compile Useful Information

✓ Obtain an understanding of the network infrastructure at each college and university.

2. Analyze Goals & Objectives

✓ Do colleges and universities have effective security policies in place?

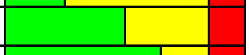
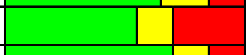
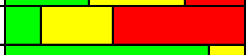
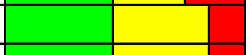
3. Review Operations

✓ Do colleges and universities enforce security policies effectively?
✓ Do colleges and universities use logon IDs and passwords properly? Are users required to change passwords periodically?
✓ Is access to network data and resources appropriately limited to faculty, staff, and students based on need?
✓ Is there sufficient protection over the physical access to network infrastructure?
✓ Do colleges and universities use adequate safeguards (e.g. virus detection software, access lists, firewalls...) to protect networks and data from unauthorized access?

4. Test Legal Compliance

✓ Do colleges and universities have policies and procedures in place to ensure that software-licensing agreements are followed?

Appendix B
MnSCU Office of Internal Auditing
System-Wide Security Risk Ratings

Information Technology Risk Measures	System-wide Rating
♦ **Network Infrastructure Documentation**	
Network administration policies and procedures are in place.	
Detailed network diagram(s) exist.	
Policies and procedures are in place and communicated to all users.	
♦ **Physical Security (1)**	
Physical access to the servers is limited.	
Physical access to wiring closets is limited.	
Physical access to hubs, switches, and routers is limited.	
Laptops not in use are stored in a secured location.	
♦ **Logical Security (1)**	
Process in place for adding users to network.	
Process in place for changing or removing user access.	
Authorized user lists are reviewed periodically.	
Administrator rights are limited.	
Administrators use separate account for daily activities.	
Password security used on servers connected to WAN.	
Users are required to change passwords periodically.	
Shared accounts are not used.	
Technology in place to manage remote access via Internet & dial-up.	
Servers are not being used as workstations.	
♦ **Backup (1)**	
Backups of data and programs are performed daily.	
Backup tapes are stored offsite in a secure location.	
Periodic test-restores are completed on backups.	
♦ **Virus Protection (1)**	
Virus protection is on all workstations and laptops.	
Virus protection is on all servers.	
Virus protection signatures are updated, as they become available.	
Updates to virus protection software signatures are automated.	
♦ **Software Licensing (1)**	
A software inventory is maintained and updated regularly.	
A process is in place for complying with licensing agreements.	

Risk Level Legend: **L - Low** **M - Medium** **H - High**

(1) The ratings relate ONLY to servers under the administration of a CIO.