Minnesota State Colleges and Universities

BOARD OF TRUSTEES
STUDY SESSION
OCTOBER 22, 2013
MCCORMICK ROOM
30 7TH STREET EAST
ST. PAUL, MN

Board of Trustees Members Present: Chair Clarence Hightower, Trustees Margaret Anderson Kelliher, Duane Benson, Alexander Cirillo, Cheryl Dickson, Dawn Erlandson, Philip Krinkie, Alfredo Oliveira, Elise Ristau

Leadership Council Representatives Present: Chancellor Steven Rosenstone, Interim Vice Chancellor Chris McCoy, Gail Olson, Office of General Counsel

Convene
The Minnesota State Colleges and Universities Board of Trustees held its meeting on October 22, 2013, 4th Floor, McCormick Room, 30 East 7th Street in St. Paul. Chair Hightower called the study session to order at 4:05 p.m.

IT Security Study Session
Chair Hightower invited Chancellor Rosenstone to introduce the Study Session on IT Security. Chancellor Rosenstone stated that the issue of IT Security is an incredibly important topic. There are responsibilities that come with this conversation. The first responsibility is the ability to share with the board the ways security is being addressed in regards to data and systems, including how the privacy and the resources in the data systems are protected. Secondly, the board is responsible for providing oversight of the work to provide IT security. Finally, the participants are responsible for engaging in this conversation in such a manner that the data and systems are protected. If a topic or inquiry arises that Interim Vice Chancellor McCoy thinks may jeopardize the security of the system, then that conversation will be taken off line. As much as the system strives for transparency, there is a responsibility to not disclose information that will undermine exactly what is being protected.

Interim Vice Chancellor McCoy stated that session would focus on IT security at the system level. He introduced Walt Swanson, Information Security Officer for the system office who will assist in answering questions that arise during the presentation.

Interim Vice Chancellor McCoy presented an IT Security PowerPoint featuring a high-level overview of the security program. The system has a talented team of security professionals that is dedicated to a standards-based practice that is constantly growing and evolving.

Interim Vice Chancellor McCoy shared that there are an estimated 1 billion cyber-attacks annually worldwide. It is estimated that one out of every three computers in the U.S. is infected with malware, and 99% are preventable.

The top five database breaches among Higher Education in 2012 were: the University of Nebraska: 654,000 (identities exposed), Indiana University: 650,000, University of North Carolina: 350,000, Arizona State University: 300,000, Northwest Florida State College: 279,000. The average cost per record breached (Higher Ed) is $142.

MnSCU processes 1.2 million business transactions monthly. There are 4.3 billion records in the Integrated Statewide Records System (ISRS) and 1.5 billion records in D2L. During peak load, 59,000 statements are processed per second. Out of 100 emails, 15 are delivered and 85 are rejected as SPAM. Across the system, over $3 million is spent annually on security.

The Information Technology (IT) division prioritizes the securing of specific, key assets such as private data on students and employees, financial transactions, intellectual property and continuity of operations.

The IT mission focuses on unauthorized use, disclosure, modification, damage or loss, by taking an active, rather than passive, approach to security; protection through intentional activity; identification and intervention; and education, training, testing and assessment. This security model is based upon a National Institute of Standards and Technology publication (800-53) on “Recommended Security Controls for Federal Information Systems.” The tactical work to safeguard the system is continuous, including testing and intervention of systems. IT Security is not “set it and forget it,” type of work.

There are four main areas of IT Security activity: first, policy, procedure, and guidelines; second, network, system, software and user controls; third, logging, monitoring, internal audit, finally, incident response, and legal framework.

The main security policy in place is Board Policy 5.23 Security and Privacy of Information Resources (5.22 also applies and deals with acceptable use of computers and information technology resources). Nine guidelines currently exist under this main policy to guide behavior within the system. Interim Vice Chancellor McCoy noted that a proposed amendment to Board Policy 5.23 Security and Privacy of Information Resources would be presented tomorrow with a second reading in November.

Network, system, software, and user controls, are the controls and technology used to operate each day. Network controls separate data traffic and to prevent unauthorized access. System controls separate data as well as separate systems from one another. Software controls maintain the integrity of the software that is installed and used. User controls separate access by user and ensure proper use of data.

Logging, monitoring, and internal audit focus on identification and response of issues. This may include monitoring the system network for suspicious activities or responding to internal audit findings that identify poorly designed or implemented controls. There is considerable growth and development in this area, especially as IT is able to respond to network conditions or database access.

Incident response and legal framework make up the fourth area of IT Security responsibilities. The system must ensure the integrity of operations and have the capabilities to recover and reconstruct activity to support the legal framework. This includes compliance with Minnesota Government Data Practices Act *(*MGDPA), Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry (PCI).

There are a number of challenges MnSCU faces when implementing a sound IT security program. Collaboration is needed to ensure the integrity, and a centralized model from St. Paul alone will not work.

Interim Vice Chancellor McCoy ended the presentation with a few questions for consideration: How is security infused into every activity? With limited resources, is the focus on the right priorities? How should the system balance the benefits of new and emerging technologies (e.g. cloud and mobile) which allow for innovation, exploration, and discovery with the risks?

Trustee Oliveira inquired if the system had experienced any breaches with the Integrated Student Record System (ISRS). Interim Vice Chancellor McCoy replied that to his knowledge that there have not been any breaches and IT continues to provide mechanisms to monitor the systems to protect the integrity of this data.

Trustee Oliveira inquired if there is a concern with ISRS since it was incorporated many years ago. Interim Vice Chancellor McCoy responded at present, there are no concerns about the age of the technology or the solution being used. It is important to separate issues of security in windows from the issues of security in a core data base solution. The system uses an integrated practice in the development of database systems. IT also uses compartmentalized access to data within these systems. The different layers work in concert to help provide the access controls to protect the system. Trustee Oliveira asked if there are concerns for programs like Hobsons that pull data from ISRS. Interim Vice Chancellor McCoy responded that in general, the systems are not connected and there are mechanisms used to transfer the data. This separation of data protects and ensures the security of the systems data.

Trustee Dickson stated that there would never be enough funding for security and with only $3 million spent on IT Security, the board should applaud the work of the people that are supporting these efforts. Interim Vice Chancellor McCoy commented that the task is daunting and the IT Security team is of the highest caliber and very dedicated. Trustee Dickson requested that Interim Vice Chancellor McCoy distinguish between the malicious activities listed on slide 5. Interim Vice Chancellor McCoy stated that the category of cybercrime generally refers to financial crime, hactivisim refers to defacing a site for a political message, cyber warfare refers to sabotage for political reasons between nations, and cyber espionage refers to stealing knowledge and trade secrets.

Chancellor Rosenstone stated that IT security is the responsibility of everyone at the colleges, universities and system office and any weak link in the chain allows a point of access that puts MnSCU’s data in jeopardy. Hiring more staff at the system office to provide IT services will not work. All of the IT professionals across the system play a role in protecting the system’s data.

Trustee Anderson Kelliher asked how much is spent across all campuses on security. Interim Vice Chancellor McCoy responded that the best estimate of what the system spends on IT Security across the entire system is $3 million. It is difficult to come up with a number because IT Security is imbedded in system administration or software development. The IT staff's daily work includes specific security elements including how code is written, development of programs, and the design of databases or networks. Trustee Anderson Kelliher stated that a cost attribution may be difficult, but it needs to be done. IT is one of the areas that can get out of control when attention is not paid to it and suggested working with Vice Chancellor King to do the cost attribution. Trustee Anderson Kelliher asked for more information on backups and where the data is stored. Interim Vice Chancellor McCoy responded that there is a considerable amount of distributed activity throughout the system. The core IT systems have a well-defined back up process and recently have been moved to the state of Minnesota's tier three Data Center. Each campus has a process for data storage, backup and recovery. CIOs are engaged in conversation and there is a CIO focus committee working on issues surrounding data storage and backup.

Trustee Anderson Kelliher said at the state level there has been a conversion to a distributed service model, which includes a state CIO that has worked well and may result in savings. This structure change provided oversight and guidance from the State CIO and Minnesota Information Technology (MNiT) to the distributed sites. Would the system benefit from a model that still allows for distributed control but has more guidance and controls like this? Interim Vice Chancellor McCoy responded that the CIOs have been working on the Service Delivery Strategy as means of identifying and collaborating opportunities throughout the state, while protecting the individuality of the campuses. This work gives consideration to how to bring IT services together on things that matter. IT is scheduled to provide a study session on the Service Delivery Strategy to the board this spring. In addition to this, the CIO community has formed the IT Risk Management Committee to discuss these types of questions. The membership of the IT Risk Committee includes representatives from the CIO community, Internal Audit, Legal Counsel and the state of Minnesota Chief Information Security Officer, Chris Buse. This group is engaged in discussions about how the system can become more cohesive in the approach used to address security and risk management.

Trustee Renier stated that several years ago the state of Minnesota made a significant investment in MnSCU to address infrastructural deficiencies and bring the system up to date in order to mitigate risks, better serve students and improve both system functionality and the security of the system. Trustee Renier asked if there has been a sufficient investment to maintain the systems infrastructure. Interim Vice Chancellor McCoy responded the $3 million dollars the system spends on security buys more than just maintenance; it also purchases new tools and systems to proactively address security needs. Star ID is one example of a project that has moved the system forward.

Trustee Renier asked if the system is focused on the right priorities in order to address the most urgent needs, given there are not enough resources to perfectly secure everything. Interim Vice Chancellor McCoy responded that the focus is on the management strategies such as protecting the right assets. The tactics used change frequently due to the nature of IT security, therefore, IT needs to address the things that are the most important to the Board and the system as a whole.

Trustee Krinkie stated that a tremendous amount of work has been done to secure the system as much as possible, but inquired if the board should be looking at a different model in regards to security management as it pertains to a centralized system platform or decentralized system. Interim Vice Chancellor McCoy responded that the geography of the system suggests that distributed model should be used in some way, meaning that the personnel have to be based across the system. In developing a cooperative and collaborative model, IT has generated a level of compliance that would be difficult to achieve following another model. Staff work together to identify what is most important and align resources to meet the needs of the priorities. The work on the individual campuses is focused on what is happening locally on the campus. It would be very difficult to implement a centralized model given the current environment including the political cultures within the system.

Trustee Krinkie inquired what the best methodology would be from a security perspective. Interim Vice Chancellor McCoy responded that IT has a fairly tight coupling with the campuses in terms of how IT provides services and helps them to establish security at the campus level. This is accomplished using a cooperative model that allows the system IT division to avoid becoming overly involved on the campus. The system IT division provides links, firewalls to the campuses, and assists the campuses in implementing the shared vulnerability management tool. This tool helps IT staff perform the security checks that need to be performed on each campus. These things are done in collaboration with the campuses.

In closing, Chair Hightower stated that Interim Vice Chancellor McCoy will work with Vice Chancellor King and others to best answer the question about the costs attributed to IT security.

Chancellor Rosenstone thanked the board for a terrific discussion. IT security is something that must be reinvented every day to respond to new challenges. This is remarkable work performed not only by the staff at the system office but by colleges and universities across entire system. Everyone must share in the high standard that must meet to ensure data security. There are both board and system policies and procedures that go back to the CIO community and there are standards that individual presidents must comply. The issue is not whether there is uniformity of standards and agreement about what needs to be accomplished, but whether MnSCU has the mechanism in place to deliver that. Chancellor Rosenstone said that given the huge variety of functions that exist across the campuses, changing to a centralized model would be difficult. The standards in place must be met and are absolutely essential.

Chair Hightower thanked the presenters and adjourned the meeting at 5:10 p.m.

Respectfully submitted,

Christine Benner, Recorder