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 to

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 [illegible]
prnt(,(y ofTd [(S2(t)-2h-1(w)5o gui)-2s529(a)128s39)-2(i))-1-sernot.

with Minnesota Government Data Practices Act *(*MGDPA), Family Educational Rights and Privacy Act (FERPA), 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 thsw 10.001 Tc -s094 Tw2 Tw2 Twn9u