Senate Committee on Information Technologies (SCIT)
November 22, 2016
Minutes of the Meeting

These minutes reflect discussion and debate at a meeting of a committee of the University of Minnesota Senate; none of the comments, conclusions, or actions reported in these minutes represents the views of, nor are they binding on, the senate, the administration, or the Board of Regents.

[**In these minutes:** Security and Infrastructure]

PRESENT: Geoffrey Ghose (chair), Nancy Carpenter, Kristin Janke, William Dana, Santiago Fernandez-Gimenez, Carlos Soria, Timothy Nicols, Al Beitz, John Butler, Bernard Gulachek, Robert Rubinyi, Michelle Driessen, Kristin Janke

REGRETS: Kate McCready, Karen Monsen, Diane Willow

ABSENT: Charles Miller, Yoichi Watanabe

GUESTS: Bernie Gulachek, interim vice president and chief information officer, Office of Information Technology (OIT); Brian Dahlin, chief information security officer, OIT

OTHERS: Vickie Courtney, University Senate Office

Chair Geoffrey Ghose welcomed the committee and the members introduced themselves.

1. Security and infrastructure - Chair Ghose introduced Bernie Gulachek, interim vice president and chief information officer, Office of Information Technology (OIT), and Brian Dahlin, chief information security officer, OIT, to provide an information security update. Gulachek began by saying that their presentation would focus on OIT information infrastructure changes that committee members may hear about this year, including the bonding measure relating to security infrastructure. Dahlin added that his presentation today would focus on five areas: security with the network upgrade, account management, security awareness and education, Two-Factor Authentication (Duo), and risk assessment.

Dahlin provided an overview of security with the network upgrade, which includes advanced intrusion detection, advanced denial of service attack defense, advanced firewalls for the data center, appropriately-sized firewalls for the general access network, and logging and security monitoring.

In the area of account management, there have been several issues with current practice identified, including staff not following the “least privilege” (no access granted beyond the needs of job) principle for Gmail and Google Docs, and the high potential of access to sensitive information by unauthorized users. Account management is a very broad conversation, Dahlin said, but the current intended scope is Google account management. The focus is to mitigate the potential access to sensitive information by unauthorized users, regulatory risk, and the security risks that may impact the University community, he added. OIT is seeking to address these issues through additional processes surrounding email access (to follow when employee status changes), Google Docs access, and creating additional security measures for identity management, including tying applications to central authentication, and upgrading the identity management system.

Regarding security awareness and education, Dahlin reported, OIT will send out monthly “Security Awareness” notices to those who use University systems, including information on how to avoid phishing scams. The phishing scam that most recently appeared, he said, initially had the appearance of coming from President Kaler, so there were employees who opened the email; this was controlled in a relatively short amount of time. Gulachek added that it is virtually impossible to prevent this type of occurrence, as individuals may sign up for Gmail accounts with any name they wish; this is one reason why OIT would like to provide increased education to the University community on how to manage their accounts. Additionally, Dahlin added, OIT would like employees to take a “Public Jobs, Private Data” course refresh.

Dahlin then provided an overview of Duo Two-Factor Authentication, which is currently in use to access Peoplesoft, but is now also available as an opt-in for employees looking for more security for their W-2’s and direct deposit information. He added that compromising an account through phishing is the number one way malicious individuals get personal information from University employees, and that the University has seen a doubling of phishing attempts in the past year. In these cases, Duo is a protective control that helps employees reduce the risk of their sensitive information being accessed once account credentials have been compromised.

Robert Rubinyi noted that a “Top Five Tips” document for account security and management may be helpful for employees, and wondered about the priority at the University for IOT devices. Dahlin responded that University Services, among others, was looking to implement service controls; OIT will work with those offices on IOT device protections.

Dahlin noted that the University and MNSCU see a relatively constant level of DDOS attacks, with some spikes. In these cases, DDOS attacks are recognized quickly, and there is a 40G cleaning mechanism for these attacks. Gulachek advised that advanced technology recognizes the characteristics of DDOS attacks, and sends them to an area where there is no danger to the larger system; the security of the network upgrade assumes attacks from inside and outside of the system. The existing system was installed in 2004. Santiago Fernandez-Gimenez asked for an explanation of the connection between Google and the proposed security solution. Dahlin replied that applications would be interconnected, with ID management required.

John Butler asked about the increased adoption of cloud-based solutions; is the University still compliant and on top of new technology? Dahlin responded that the University was still immature in this area, while at the policy level, the University is more effective than in previous years. Contracts are reviewed with an eye to the issue of sensitive data, including risk assessments, internal audit review of vendors, and third party review of vendors. Gulachek added that when contracts come up for renewal, new standards can be applied; the industry now recognizes capabilities and adds language into their offerings. Dahlin said that in the area of cloud solutions, businesses have very tight controls in place; there is an increasing need for cloud solution vendors to handle an increasing level of sensitive data.

Ghose asked about Google Drive/Docs, and the security risks inherent in using them for educational purposes; for example, he said, the default sharing settings on Google Docs are set to "anyone at the University can access." Dahlin responded that a broad risk-based assessment was performed, which can be used in helping users determine the risks; the University may also need to put additional requirements in place. William Dana asked about security issues in Google Hangouts. Dahlin responded that there may be issues discussing HIPAA-protected information over Hangouts, but that the University does not have specific controls in this area. William Dana asked about the possibility of moving to one University system, rather than having four to five options. Dahlin responded that yes, OIT has been discussing this option.

Fernandez-Gimenez asked if a central staff group could handle permissions for Google Drive folders and documents to mitigate security concerns, as is done with Peoplesoft access. Dahlin replied that while this is being discussed, the current structure is organic, which is one of its advantages; OIT would be cautious in recommending this change.

John Butler asked how the University is able to influence Google to better address the specific needs of the University. Dahlin responded that the team in OIT can make certain configuration choices, noting, however, that Google is large and not generally customizable. Gulachek added that there was much due diligence in this area before hiring Google; while more education surrounding the "share" function will be helpful for the University community, account management issues are one of the more frequently cited issues by auditors. This area needs better management by supervisors, he said, similar to getting office keys, a laptop, etc.; managers should be more careful in managing the digital environment. OIT may need to rethink provisioning policy in this area, he added, to provide more guidance on what information faculty, staff, and students should have access to. While additional requirements may seem stringent or onerous, not having them in place may put the institution at risk. These are active discussions, Gulachek added, and OIT is currently forming recommendations.

Michelle Driessen asked for more information about the new opt-in to Duo Two-Factor Authentication. Gulachek provided an overview of the issue, noting that opting in protects employees against identity theft, since the system cannot tell the difference between you logging in or someone else logging in with your password. The time it takes to enroll in Two Factor Authentication pales in comparison to the time an employee will spend if their identity is stolen, he added. Currently, opting in is not mandatory; he hopes that people at the University see the value in protecting their personal information. Driessen asked what the response had been thus far to opting in to Two Factor Authentication. Gulachek responded that 15% of those paid through Peoplesoft had enrolled, which is about 7,300 people; he asked members of the committee to advise those in their units to sign up. Rubinyi noted that when he went to sign up for Two Factor, the tutorials linked in the email from OIT were not accurate. Gulachek responded that OIT Communications had re-worked the tutorials and that the revised tutorials were now posted. Dahlin clarified that the complicated process in signing up for Two Factor was intentional, because if it was made too easy, malicious users would be able to sign up as authorized users.

William Dana asked if SCIT should take any action on this item. Dahlin noted that there is a current policy in place for Two-Factor Authentication relating to the highest-risk applications, though the policy doesn’t address individuals. Gulachek confirmed that individual use of one’s own private data is not covered under any policy requirements. Al Beitz asked the committee if they felt this should be discussed at an upcoming Faculty Senate meeting. Ghose responded that perhaps the committee could write recommendations that this information be included in unit HR onboarding for new employees. William Dana asked if data security was currently included in the curriculum, and if not, how it may be better built into the core fabric of courses.

Rubinyi asked about third-party applications used by faculty, and how these are managed. Dahlin responded that vendor contracts require that companies notify the University of any breach; the University then works with the vendor to resolve the issues. This becomes very challenging if the vendor is not a contract vendor, since the University would not necessarily be notified of a breach. OIT can provide guidelines to faculty signing up for these applications. Gulachek added that users in this instance need to know what type of data they have and what the requirements are for that type of data. Ghose asked if there was a central place to discuss the use of third-party apps for his classes. Dahlin replied that yes, OIT can review these apps from a security perspective. Gulachek added that the annual IT governance process can identify needs not currently being met. Depending on the scale and use, faculty can call 1-HELP or speak with their academic technologist about these issues.

Hearing no further business, the meeting was adjourned.

Barbara Irish
University Senate Office