THE UNIVERSITY OF UTAH®

SUMMARY FOR ARCHITECTURE & NEW TECHNOLOGY COMMITTEE

DATE: May 23, 2016

TIME: 10:00 a.m. – 12:00 p.m.

LOCATION: Dumke Room, Eccles Broadcast Center

IN ATTENDANCE:

David Blackburn
Mark Beekhuizen
Pieter Bowman
Tim Ebner
Jeff Folsom
Demian Hanks
Matt Irsik
Sylvia Jessen
Josna Kotturappa
Jim Livingston
Chris Roberts
Steven Seal
Jon Thomas
Daniel Trentman
Rob White
Thomas Wolfe

COMMITTEE SUPPORT: Scott Sherman

UNABLE TO ATTEND:

Joe Breen
Rebwar Baesmat
Derick Bingman
Dean Church
Matt Harting
Jim Logue
Chris Stucker
Wes Tolman

AGENDA ITEMS DISCUSSED:

- Current and upcoming security issues for data/network/IAM
- Certificate management
- Active Directory discussion
- Governance submission web form approval
- Debrief of Deloitte IT assessment findings on architecture issues
- Campus-wide IT strategic plan
- Campus IT financial model statement of work
- Network connection memorandum of understanding

Current and upcoming security issues for data/network/IAM

Chief Information Security Officer Dan Bowden first presented an informational overview of security news and threats. Recently the U.S. Department of Health & Human Services' Office of Civil Rights (OCR) has been contacting a number of HIPAA-covered entities to perform routine HIPAA audits. At this point, the University has not yet been contacted and has not been identified as one participating in the 2016 effort. The focus of the audit is policies, procedures, risk management, and administrative safeguards. Bowden said he believes the University is ready for an audit if we are contacted. He reminded the group about the new information security policies and supporting rules, and said that they're now digging down into the procedures for each department/organization at the U. Additionally, the Information Security Office is continuously working on technical safeguards, including Identity and Access Management (IAM), endpoint security, two-factor authentication (2FA), anti-malware, security operations and incident management, and business associates/third parties.

On FERPA/student data: ISO has defined three categories of data: restricted, sensitive, and public. Today, they have categorized student data as Sensitive (strongly recommended to be encrypted, but not required). Currently there are no specific data security requirements associated with FERPA. If the University were to make student data Restricted, there would be many compliance requirements to be met. In the next 12 months, ISO will talk to key parties (including the registrar and Academic Senate faculty committee) and ask if those groups would like to revisit making student data Restricted, bearing in mind that there would be a wide impact if this happened.

On PCI: Bowden explained that Payment Card Industry standards are now a large focus because Wells Fargo changed the University's merchant categorization, so the strategy has been scope reduction and encryption. ISO recently completed the second formal report on compliance, and Bowden said that if PCI stays on track, it is slowly evolving towards a low-risk domain.

On endpoint security: At any given time, the security team has about 90 incidents that have been escalated to requiring investigation. Bowden explained that hackers have learned there is more success with attacking individual users and devices than systems, and because of that there is a higher risk for a data breach. The current problems are dwell time (how long after malware hits before ISO realizes it's there), forensics, and massive backlog. There is a lack of visibility and capability to quickly address compromised hosts (personal devices). ISO's plan is to purchase advanced endpoint security agents and get those deployed during the remainder of the calendar year (2016).

On 24x7 security operation center: ISO is awaiting final budget approval to transition to 24x7 security operations in support of the hospital (i.e. anything affecting clinical networks, devices, and users). That is the short-term scope – future areas to be determined. The goal is to implement by the end of 2016.

On 2FA: Today there are two options being deployed for two-factor authentication (2FA); RSA is being used for Citrix and DUO is being used for CAS. Not every 2FA solution is certified for every single application used on campus and hospital, which is why there are two solutions used today. Bowden said there is no bias toward or against either, and that a third solution may arise. ISO plans to get all of campus/hospital using their respective solutions (DUO, RSA) by the end of 2016, with further testing and rollout in 2017.

On IAM: Streamlining the provisioning and de-provisioning of access will be handled by a new IAM platform. The initial scope to address is high-risk systems (Epic, PeopleSoft, Kronos, etc.). Two phases have been identified (access certifications and automating ULM, access requirement, and password management). The first goal was to define the scope and pick a platform. That has been completed (SailPoint was selected as the platform). ISO recently completed an RFP for consulting services to implement SailPoint.

Certificate management

Certificates are known to be a contributing weaknesses to most large-scale breaches. In a big breach scenario, if a user's credentials are compromised, a hacker can potentially get access to a certificate authority and take over the user's certificates. When that happens, the hacker can then encrypt all of his/her activity on the network. At this time there is no central management plan around certificates. Bowden recommended ISO or another group should be assigned to be the central certificate management authority, and that there are tools to be looked at that manage certificates automatically. The group discussed and it was agreed that it would be wise to take the decision of who should manage certificates to an ad hoc group. The committee moved to do so. The details of the ad hoc group will be defined over email.

Active Directory discussion

Bowden said this is more than just a security effort. AD has become a common platform that University departments/organizations have used as each have determined necessary (building separate AD instances for anything "important"). There hasn't been a strategy defining parameters for AD usage, which has led to security and compliance issues. The goal now is to create a better end-user experience and a better IT management platform. "Zero day" provisioning and management was discussed, including Microsoft's AD platform. The Microsoft solution would provide a lot of capabilities and other security tools that would benefit the entire campus. This common platform would give anyone the authority to manage the assets in one's area or department, as well as create better visibility to account for assets and secure them. ISO is currently exploring options, including directory consolidation, and has an engagement with Microsoft as well as budget funds set aside (pending FY17 budget approval). Bowden's recommendation was to continue moving forward with the identified plan. The committee discussed and agreed that ISO should continue with the current plan, and continue working with groups on campus as progress is made.

Governance submission web form approval

Scott Sherman, the IT governance liaison and special assistant to the chief information officer, presented three web forms for submitting requests to the new governance groups. There were no recommendations for any changes to the forms, and the committee moved to approve the forms as-is.

Debrief of Deloitte IT assessment findings on architecture issues

Chief Technology Officer Jim Livingston presented on Deloitte's findings, specifically as they relate to architecture. Livingston said the most meaningful slide from the Deloitte presentation was the U's Business Requirements for IT. It showed the U's stakeholders have a variety of business requirements that aren't being addressed by the U's current IT operating model. Livingston stressed that we have to work more cohesively as a campus to solve some of these issues, and that an environment must be built that is competitive and entices students/researchers/patients/etc. to come to the U. Deloitte says there are three pillars to focus on: 1) strengthen the core, 2) increase alignment between UIT and college department IT to operate collaboratively, and 3) innovate and transform. Livingston said architecture is what is going to help bring this together and bring closer alignment. Specific problems were discussed, including the lack of a University architecture and standard business processes, limited integration and standardization of the U's systems, silos, and no IT lifecycle management. Going forward, infrastructure and the technical architecture will be the initial focus. Campus network services are not currently meeting the demands of the U. Our network reliability is lower than other leading organizations. The process to establish an IT architecture team is already underway. Livingston reiterated that these are tough issues to solve, and that we must come together and work cohesively and collaboratively. There were no questions from the committee.

Campus-wide IT strategic plan

Chief Information Officer Steve Hess presented on two strategic plans. The first was the UIT strategic plan. Hess went over UIT values and how they relate to the recommendations from Deloitte. He covered the goals within each of the five defined IT strategic goals (support faculty and student success, advance research computing, support health care, promote campus efficiencies and effectiveness, and strengthen internal operations). Every employee in UIT has been evaluated and some are being reassigned based on their core strengths. There was no action item or vote on this plan.

The second plan Hess covered was the overarching University of Utah IT strategic plan. It showed the current state and problems that exist, along with seven top IT initiative categories (governance, finance, infrastructure, security, enterprise applications and integrations, people, and processes) and projects to be completed or started on within the calendar year. He asked the committee for any changes or suggestions to this plan; there were none. The committee voted to approve the plan as-is.

Campus IT financial model statement of work

University Information Technology Chief Finance Officer Lisa Kuhn and Steve Hess explained how this finance project will address two recommendations from the Deloitte assessment: mature the funding model to align to ubiquitous services, and develop a ubiquitous service strategy. They've put together a group to work on the project that includes a good representation of hospital and campus people who primarily focus on and understand finances. The current issue is that IT is not funded to the extent that it needs to be, but the administration does not feel inclined to fund it more until there is a current state assessment. Phase 1 of the project will be just that – identifying services, costs, and funding flows. The goal for completion is October 2016. The committee voted to approve Phase 1 to move forward with the assessment.

Network connection memorandum of understanding

Jim Livingston presented a proposed network connection agreement draft to the committee. He said this is a common practice of large organizations. If a group or department is going to connect something to the network, which is a shared resource, there are certain rules and obligations to follow. This is becoming a larger issue in light of the Internet of Things; more and more devices are being connected to the network, some of which we don't even know are out there. There are security implications as well as major effects on the network performance.

The purpose of the agreement is for the user/group/department to show they are a valid University entity; to agree that they won't broadcast information that compromises the wireless environment; to verify they will address items such as patches and vulnerabilities on their servers or other devices; and to assert they are not introducing vulnerabilities or threats to the organization. Livingston said we are trying to create a more collaborative environment where we can work together on how we utilize the devices connected to the network.

Livingston said one committee member has already seen the draft and sent revisions suggesting more collaborative verbiage, and a few other members voiced agreement with those revisions. Due to their complexity, along with other questions raised, the committee agreed to put together an ad hoc group to discuss those revisions and details and formalize a new draft. The committee voted to approve the ad hoc group, and Trevor Long was put in charge of pulling together the group.

Action summary			
Action	**Topic**	**Person/Group**	**Next step**
Approved	Certificate management ad hoc group	Portfolio	The ad hoc group will meet to determine what group or department should be in charge of certificate management.
Approved	New governance submission web forms	Portfolio	Continual improvement of the forms as needed.
Approved	University of Utah IT Strategic Plan	Portfolio	The plan will move forward as outlined in the document.
Approved	Service finance project – Phase 1	Portfolio	The finance project group will move forward with Phase 1 of identifying services, costs, and funding flows.
Approved	Network connection memorandum ad hoc group	Portfolio	Trevor Long will pull together the ad hoc group to discuss revisions and edits and create a new draft of the memorandum.