SUMMARY FOR ARCHITECTURE & NEW TECHNOLOGY COMMITTEE

DATE: September 26, 2016
TIME: 10 a.m. – 12 p.m.
LOCATION: Dumke Room, Eccles Broadcast Center

IN ATTENDANCE:

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

COMMITTEE SUPPORT: Scott Sherman, Emily Rushton

UNABLE TO ATTEND:

Rebwar Baesmat	Derick Bingman	David Blackburn	Joe Breen
Dean Church	Demian Hanks	Matt Harting	Jim Logue
Wes Tolman			

AGENDA ITEMS DISCUSSED:

- Network architecture community of practice
- SMTP authentication/email relay changes
- Open floor

Network architecture community of practice

Chief Technology Officer Jim Livingston reminded the committee that one of the charges from the Deloitte assessment is that the University needs architecture standards across campus, and he said the best way to achieve these standards could be through a collaborative community of practice.

Clayton Barlow, associate director for Enterprise Architecture, took over and explained that one challenge that has been immediately recognized is a lack of architectural methods, processes, and definitions. A community of practice would present an opportunity to work together with people who fulfill an architecture role on campus, as well as bring some continuity to the practice, which will allow the group to begin developing true architectural standards that the entire university can abide by. Barlow clarified that the group would be looking for outcomes and solutions from a business perspective, and not a technical perspective. The proposed formation of the network architecture community of practice would bring together staff on campus who fill a network architect role to grow the skillset of architects on campus, and to discuss standards that should drive the campus network architecture in the future. The community of practice would present recommendations to the ANTC for approval as necessary. Barlow asked the committee to approve the formation of a network architecture community of practice.

There was some discussion on how the committee would be selected, and Barlow clarified that it will be invite-based, and asked for suggestions from the ANTC on who should be part of the committee, with a few requirements listed such as willing to engage, strong documentation skills, comfortable being coached and mentored as well as providing coaching and mentoring, and so on. CIO Steve Hess commented that he strongly supported the idea. One committee member asked about metrics, and Livingston said his expectation is the group would come up with specific metrics for measuring success during the process of establishing architectural standards.

The committee voted to approve the formation of the network architecture community of practice.

SMTP authentication/email relay changes

Chief Technology Officer Jim Livingston recapped a change that was recently made to the U's email system to turn off off-campus authentication to SMTP servers. The change was made due to a problem of spammers utilizing compromised accounts to send thousands of emails. The U's reputation score started to lower, which increased the probability of being blacklisted. A critical point was reached during the start of Fall 2016 semester when the UMail team noticed an increased number of compromised accounts sending out spam. Livingston explained that this happens because SMTP is inherently insecure and allows an infinite number of attempts to authenticate, which opens up the University to brute-force attacks.

Before immediately shutting down off-campus authentication to SMTP, a few things were tried: increasing the level of monitoring and decreasing the number of emails that can be sent from a certain account in a certain timeframe. Ultimately these solutions were not effective enough, and the decision was made to shut down outside authentication to SMTP (with the exception of a few whitelisted services, such as @TheU and ServiceNow). This resulted in a minor effect for about 1,000 users who are no longer able to use certain older email clients off campus unless connected to VPN.

Upon making this change, the U's reputation score improved dramatically. There are no more compromised accounts, and the number of concerns overall was very low – less than 10 trouble tickets to the help desk.

One member asked why the UMail team hasn't addressed this problem earlier, and pointed out that the problem is actually compromised accounts, not SMTP. Interim Chief Information Security Officer Corey Roach stepped in and agreed that compromised accounts due to weak passwords are the core of the problem. The Information Security Officer is currently working on forcing bad passwords to be reset, as well as rolling out two-factor authentication for all University employees.

There was more discussion regarding SMTP and the scale of the problem, with Common Infrastructure Services/Unified Communications Director Mike Ekstrom re-explaining the reasons why SMTP needed

to be shut off. Livingston added that this was a very good example of why the University is implementing a network architecture community of practice. Livingston also addressed a point in regards to the communication and timing, and the reason why the change happened so swiftly (because the reputation score had dropped so drastically and quickly).

There was no further discussion. This was an information-only item.

Open floor

There were no open floor topics discussed.

Action summary			
Action	**Topic**	**Person/Group**	**Next step**
Approved	Network Architecture Community of Practice	Portfolio	ANTC members are asked to suggest individuals they feel would be a good fit to join the community of practice, based on a list of characteristics offered by Clayton Barlow.