

**SUMMARY FOR STRATEGIC INFORMATION TECHNOLOGY COMMITTEE**

**DATE: May 15, 2018**

**TIME: 1:00 p.m. – 2:45 p.m.**

**LOCATION: Administration Boardroom, Marriott Library**

**IN ATTENDANCE:**

Randy Arvay	Holly Christmas	Steve Hess	Demian Hanks
Harish Maringanti	Ken Nye	Cory Stokes	Rob White
Amy Wildermuth			

**COMMITTEE SUPPORT:** Jesse Drake, Emily Rushton

**UNABLE TO ATTEND:**

Cathy Anderson	Melissa Bernstein	Kirsten Butcher	James Elder
Aaron Fogelson	Bo Foreman	James Herron	John Horel
Jakob Jensen	Mike Kirby	Nancy Lombardo	Andrew Olson
Mary Parker	Kevin Runolfson	Ryan Smith	Rick Smith
Jess Taverna	Jim Turnbull	Howard Weeks	Jeff West
Joanna Yaffe			

**AGENDA ITEMS DISCUSSED:**

- Review IT governance voting structure changes
- SMTP security path forward
- Campus-wide customer relationship management
- Regulations for enterprise software
- IT risk governance
- Open floor

**Review IT governance voting structure changes**

SITC Chair Amy Wildermuth led a brief discussion on the current IT governance voting structure, noting an uptick in attendance since the meeting moved from Eccles Broadcast Center to the Park Building. Demian Hanks, IT director at the College of Social & Behavioral Science, proposed voting by email as a way to boost participation, and advocated for contacting members as new information emerges. Chief Information Officer Steve Hess noted that his office makes a concerted effort to publish agendas as far in advance of meetings as possible, and welcomes questions or comments at any point. Holly Christmas, web developer in the College of Fine Arts, inquired about the committee’s stance on a representative voting structure. Hess said the committee will accept the vote of a representative on behalf of an absentee member, and Wildermuth added that if a vote is anticipated, absentee members may cast their vote in advance.

The committee approved continuing the current voting model for an additional year before revisiting the results again.

**SMTP security path forward**

Mike Ekstrom, director of UIT Network and Communications Infrastructure, presented an update on the

university's continuing efforts to restrict Simple Mail Transfer Protocol (SMTP) emails. SMTP is an internet standard for email transmission known to be an inherently insecure phishing and SPAM attack vector. Malicious campaigns are known to utilize compromised SMTP accounts, and in some cases, spoof an email account. Chief Information Security Officer Randy Arvay noted that a single user compromised via email can put an entire department at risk.

Ekstrom presented figures from UIT's Information Security Office indicating that in the previous week, it blocked approximately 12 million email threats out of 16 million received – 879,000 of which were SPAM, 1,900 which were identified as phishing emails. Wildermuth asked if blocking 75 percent of emails is unusual. Arvay said it's actually not uncommon for large organizations like a university to block 90 percent of emails.

Ekstrom proposed a new method for SMTP mail system exchange on the internet that includes: Requiring all outbound and inbound SMTP to flow via smtp.utah.edu, and blocking all other inbound and outbound SMTP email. While there is a risk of impacting unknown email servers, unique mail forwarding emails, and "false positives" where an innocuous email is identified as malicious, Ekstrom said that all can be addressed through collaboration. Arvay added that the likelihood is very low, and the security risk compels action. The proposal has already been approved by the Architecture and New Technology Committee, and Ekstrom said that UIT is working to identify any legitimate email servers which could be impacted. Next steps are to gather more information from stakeholders and technicians, as well as to create and execute a robust communication campaign.

After some discussion, the committee voted to approve targeting July 15, 2018 as the change date, but no later than August 10, 2018.

### **Campus-wide customer relationship management**

CIO Steve Hess addressed the pressing need for a customer/constituent relationship management (CRM) strategy at the university. In higher education, CRM software applications aggregate relevant personal information of constituents (prospective and current students, staff, alumni, donors, etc.) across different channels into a single database for the purpose of automating and managing communications.

Hess said that a campus-wide CRM would facilitate better decision-making and reduce data silos. By its own account, Hess said that the cloud-based CRM Salesforce identified up to 18 instances of its platform currently in use at the university. A more centralized CRM will help the university personalize education, which he called critical to bringing more students to campus and guiding them from admissions through graduation and beyond.

Hess proposed the formation of an ad-hoc sub-committee to look at strategically utilizing CRM on campus. The committee voted to move forward with its formation.

### **Regulations for enterprise software**

Deputy CIO Ken Pink informed committee members that in 2017, University Support Services (USS) staff spent more than 10,000 hours integrating software purchased by campus entities into PeopleSoft, which equates to 10 to 15 percent of USS's financial resources and 65 percent of work hours dedicated solely to software maintenance. He said that in commercial industries, 50 percent is considered an absolute tipping point.

Pink shared the draft of an enterprise software policy aimed at increasing transparency around purchases and “delivered functionality” (e.g., not buying software that the university already owns), ensuring that USS and the Information Security Office (ISO) are engaged earlier, new software can in fact integrate with PeopleSoft, and that the true cost of ownership is captured (i.e., services provided by USS are not entirely free). The policy would apply to campus and Hospitals/Clinics, but not patient care.

Pink said USS engaged with the university’s Purchasing department a year ago to gain visibility into RFPs related to software, allowing USS to reach out to purchasing units and inform them of the expectations outlined above. UIT also rolled out an Application Programming Interface (API) strategy intent on publishing a set of role-based API standards for public and private vendors seeking to securely integrate data with PeopleSoft.

Cory Stokes, UOnline director and associate dean for Undergraduate Studies, advised any software policy decisions to involve faculty members. Wildermuth noted that some level of exception should be weighed for low-level applications that don’t integrate with PeopleSoft, for which a formal approval process would be overly burdensome. Wildermuth also pointed out that the definition in the policy should be rewritten, among other things.

After further discussion, the committee endorsed and approved the concept (though not necessarily the draft in its current form) of moving forward with a policy addressing this issue.

### **IT risk governance**

CISO Arvay sought the committee’s input on risk at the university relating to technology deployments. ISO has mitigating technical controls in place, but Arvay said that overall, purchase decisions tend to be disparate and resource-driven, where security and risk governance are an afterthought, and exceptions invoked during the process often lead to additional risk.

Arvay asked if SITC is the appropriate group to approve or deny IT solutions that add risk cost to the university, what exceptions currently exist, and whether this issue would be best explored by a broader group which would give him institutional-backing when approaching an individual or unit whose actions (or inactions, as in the case of not installing software updates) present an excessive security risk.

Wildermuth suggested forming a sub-committee that reports to SITC, and draws stakeholders from existing IT governance committees. Hess recommended calling on representation from the Office of General Counsel and Risk and Insurance Services. Arvay said he would solicit for members and asked anyone interested in serving to contact him directly.

Arvay also gave a brief overview of the European Union-based General Data Protection Regulation (GDPR), which changes requirements for companies that collect, store or process large amounts of information on residents of the EU. Arvay said that GDPR-related messaging has been prepared, and data storage systems are being assessed. While universities in the United States are not the targets of the measure, they are required to assign a Data Protection Officer (DPO).

The committee voted to make Arvay the University of Utah’s DPO.

**Open floor**

Earlier in the meeting, Hess introduced Emily Rushton, newly-named Special Assistant to the CIO. Hess and fellow committee members also thanked Wildermuth for her service and stewardship of SITC since its inception in 2016. Wildermuth is vacating her role as committee chair after being named dean of the University of Pittsburgh School of Law. After some words of gratitude, Hess presented a card signed by fellow committee members, while Pink presented Wildermuth with two pens and a wooden box – all handmade. The pens bore the colors and logos of the U and Pitt, respectively.

<b>Action summary</b>			
<b>Action</b>	<b>Topic</b>	<b>Person/Group</b>	<b>Next steps</b>
Approved	IT governance voting structure	SITC	Continue current voting model for another year.
Approved	New method for SMTP email exchange	SITC	Gather information from stakeholders and technicians; execute communication campaign. Change target date is July 15, 2018.
Approved	Sub-committee to explore campus CRM	SITC	Reach out to prospective candidates.
Approved	Enterprise software policy	Ken Pink	Take feedback from this SITC meeting and create a second draft to be vetted in a future SITC meeting.
Approved	Sub-committee on IT risk governance	Randy Arvay	Reach out to prospective members.
Approved	Data Protection Officer	Randy Arvay	Take on the responsibilities of DOP due to new GDPR standards.