Minutes
CIO Advisory Committee Meeting
The University of Tennessee Health Science Center
910 Madison, Room 502
February 24, 2014

Members Present (12): Larry Tague (Chair), Bob Belland, Yan Cui, Charles Cossar, Paul Gahn, Sajeesh Kumar, La’Keith Miller, Anna Montgomery, C. Judith Nyabando and Tricia Page; Adobe Connect: Jackie Burchum and Jada Williams

IT Services (ITS): Jan van der Aa, Vice Chancellor for Information Technology and CIO; Judy Jefferson Johnson, Secretary; Vikki Massey, Project Manager

Absent (5): Jim Eoff, Paul Dassow (Chattanooga), Rakesh Patel, Vada Singleton and Travis Turner (Knoxville)

Mediasite Recording: The recording of the 2-24-2014 meeting is provided for members’ review.

Meeting Materials: Agenda; Minutes of the January 27, 2014 meeting.

Call to Order: The meeting was opened by Chair Larry Tague at 9:00 a.m. It was motioned, seconded and unanimously voted to accept the agenda. A quorum was met by the membership in Blackboard to approve the January meeting minutes.

ITS Reports
Blog Updates (Tague): ITS directors have posted new reports. Members were reminded to review these reports and add comments, if any.

OLD BUSINESS
IT Goals and Priorities (Tague): There has not been a lot of activity from any of the subcommittees relative to the updated IT Priorities list and new goals and priorities.

- Subcommittees Membership: To promote more discussions in subcommittees, it was motioned, seconded, and unanimously voted to add individuals on campus who are very knowledgeable in IT affairs and want a voice in IT discussions to the subcommittees. They will not have a vote.

- Google Apps: Google has agreed to sign a BAA HIPAA Agreement. This may provide a possibility to add Google Apps (a suite of applications and collaborative instruments) to current campus resources. It was motioned, seconded and unanimously voted to form a Google Apps Subcommittee to research the benefits in determining how the apps could apply to our campus, the possible savings, and if it would be beneficial to bring Google Apps onto campus.

  - Google Fiber: With current technology available and advances in information technology transmission, Tague discussed the need for faster internet speed in transmitting x-ray images, etc. To drive this initiative, IT Services needs to be at the table to secure this service for UTHSC that would facilitate moving data sets around within the city. Applying for Google Fiber is the first step. This is a City of Memphis rather than UTHSC initiative.

Vision for Information Technology on the UTHSC Campus (Tague): Survey results for possible vision statements for IT are posted on Blackboard (see also the agenda). Only 8 votes were received (5 for version 1; 3 for version 2). More feedback is needed from the committee and from ITS members. The survey is still posted under the Announcements navigation link. Additional feedback:

Minutes 2/24/14_apprv’d 3/24/14
• Use one statement for the Advisory Committee and the other for the campus mission statement. Version 2 needs to be shortened. (IT vision for campus needs to be innovative.)
• A vision statement meets stated goals. IT Services (ITS) functions that serve the campus must have goals that focus on campus goals for IT, and interface with the campus mission.
• The campus mission statement needs to include the active partnership of ITS to campus in providing the support or interface in achieving its overarching mission.
• The proposed statements need to show the relationship of the committee as an advisory body to ITS. Action Item: Tague will add this to the first proposed vision statement.
• ITS mission statement: “To act as a catalyst for change and innovation and deliver information technology that enables and facilitates discovery to achieve excellence in patient care, education, research, and community service.” Vikki Massey will post it on Blackboard.

Action Item: Vice Chair Paul Gahn suggested re-reading the vision statement for ITS and refocus on the vision statement that needs to be written.

ROI (Return of Investment) for IT Services: CIO van der Aa wants ITS to eventually have an online service catalog that includes associated costs (services provided, cost of the services, who provides/uses the services). This will help in making informed decisions about software and services. The ITS software budget is currently $800K for software/hardware purchases, license fees, maintenance costs (Microsoft Office Suite free to campus, Banner, Oracle, the MathLab, SPSS and some others).
• First step—software inventory. With user-utilization, this will determine whether a campus license is needed, or if a single user’s license would serve the purpose. Tague noted all campus software purchases should be included in this evaluation process.

NEW BUSINESS
BerryDunn IT Security Posture Assessment Report (van der Aa)
• The security assessment requested by the UT Board of Trustees last fall was done UT System-wide. Recommendations were derived from assessments from all campuses and compiled into the report. (The entire document could not be shared.)
• A handout of the 14 recommendations from the report was distributed for review. Action Item: van der Aa will email the handout to remote members and post it on Blackboard.
• Framework models for assessing IT security matureness of organizations are NIST and COBIT. Overview highlights of the consultants’ recommendations:
  1. Policy Authority and Enforcement Standards
     a. NIST: Initially used. Policies, standards and procedures had to be well-established, in place, documented and disseminated; otherwise 0, the first level, is applied. All campuses would have received 0 as this is not consistently done. The score therefore was not helpful if trying to achieve security matureness.
     b. Modified COBIT: This model based on a 0-5 scale was used—provides some insight on our current levels. On a graded scale, HSC scored 2.3, the highest System-wide.
  2. Roles and Responsibility: Recommendation—Strengthen Maturity. It reads, “The University needs to redefine the CIO position of the University System (System level). The position will have broad oversight of security and other IT functions. Each campus should have a reporting relationship to both campus leadership and the System CIO.” van der Aa noted an assessment was done a few years ago that addressed this. No need to redo it. He has some concerns about this recommendation. Also noted, some introspection needs to be made available for those who will be working the recommendations.
3. Staffing Levels: System-wide concern. On average, 5% of total IT force should be dedicated to Security tasks. Each campus has at least one dedicated staff, except UT System with 8 FTEs (more than all campuses combined). UTHSC with 75 staff should have 4 Security FTEs. Currently, two positions are open and one was filled for a total of 3 FTEs.

4. Strategic IT Planning: The recommendation—need to be better.

5. Training and Awareness: UTHSC has made significant progress in training this year with HIPAA information security and privacy training. Several campus areas have a compliance level of 100% – a perfect score, including Facilities with a diverse staff (administrative, custodial and high-skilled workers). All campus areas should attain 100%. Recommendation: need to pay more attention to this area.

6. Risk Management: UTHSC does not manage risks very well. Our risks are not always known, and how can we manage our risks.

7. Data Ownership: There is not always a clear understanding of who owns the data, how the data is classified, what is the importance of this data, are SSNs important, also TN unique ID numbers—are they also protected and does anyone know theirs?

8. Incident Response: UTHSC is very reactive, if we have an incident. This is a 7-step process. We need to establish how we respond to incidents, whether real or perceived.

9. Patch and Vulnerability Management: UTHSC makes a real effort to keep systems patched and up-to-date. If we can no longer do so, if vendors no longer support operating systems (such as Microsoft XP—will end 4/8/14), UTHSC needs to have plans to address upgrading or replacing the systems. Noted: Sophos works with XP. XP can no longer be patched.

10. Software Development Life Cycle: Not sure why software was singled out. All products purchased including hardware, and software purchased or developed—all have life cycles.

11. Disaster Recovery: Plans need to be written, documented, tested and regularly executed. This is a big area where recommendations were made.

12. Access Management: Ties into identity and access management (IAM). Access should be on a need-to-know basis by those who are trustworthy and have proper credentials.

13. Network Security: Feel pretty good about our network security. We work hard to keep our environment safe.

14. Physical and Environmental Protection: Confident about the physical level of security with card reader access to campus buildings.

Next Steps: Deadlines need to be met:
1. April 1st: Develop a plan to meet the above recommendations. A plan also needs to be developed to address campus-specific observations identified (not distributed).
2. May: Report due to the Audit Committee for the Board of Trustees meeting.

Action Item(s):
- Members should review the distributed summary handout and add their thoughts, suggestions and/or feedback on Blackboard or email van der Aa at vandera@uthsc.edu.
- Tague will create a Discussion Board in Blackboard.

van der Aa’s overall perspective—the BerryDunn assessment was fair, but not perfect. UTHSC is already rectifying a number of the items, including developing policies and installing disaster recovery capabilities (storage).

Questions and Answers
Q: Are there items on the campus-specific list that need to be brought to the Committee’s attention?
A: No, not anything that has not already been covered in the overall recommendations.
Q: Has the generator’s ability to maintain the system been tested without power to the 7th Floor Alexander Building?
A: Yes, it is tested once a week. Also, generator testing is done on a regular basis.

**Other Items:**

Next Meeting: **March 24th.** Tague will be out of town. Vice Chair Paul Gahn will chair the meeting.

With no further business, a motion was made and seconded to adjourn. With a unanimous vote, the meeting adjourned at 10:17 a.m.