

ITCC Minutes January 9, 2013

Meeting called to order at 4 PM

Attending: Don Wunsch, Maggie Trish Deanne Jackson, Daniel Tauritz, John Bax, Thomas Vojta, Max Tohline (for Bob Cesario), Vincent Yu, Andreas Eckert, Karl Lutzen

Approval of last two meetings' minutes (previously sent and attached) Approved.

PeopleSoft Update

Deanne Jackson: About to go through "fit gap" – check whether the upgrade and modifications are meeting our needs. Federal regulations are top priorities, UM System mandates next, Campus policies next, ease of use next. These must be approved by all four campuses. She reached out to students and faculty advisors, especially freshman year advisors to assess usability when the system was being prepared for configuration.

It was pointed out that the ITCC is willing to help with such processes in the future. That is likely to get a more representative cross-section of feedback.

Three big modules are controlled solely in Columbia, so those interested in providing input should reach out to PeopleSoft Student, HR, and Finance. These are different functional user groups, not reporting through Missouri S&T IT. There exist some complaints – that's to be expected with any new system. Removing an advising hold is one of the common ones, and they know we want this changed. We do faculty advising of students here so our needs are unique. It would not be surprising if other campuses aren't as affected but our students are advised by faculty, which is a source of institutional pride. Other PeopleSoft modifications such as grade approval are underway.

Computer Security Incident follow-up discussion and Faculty Senate referral

The Faculty Senate directs RP&A to meet with ITCC and review whether there are adequate means to insure IT provides adequate faculty computer support.

Related to this please see the attached list of security related items everyone needs to know. Some of these will merit discussion at future ITCC meetings.

The specific concerns that were raised by an individual at the Faculty Senate meeting have been thoroughly dealt with through discussions between IT and that individual. There remains an issue regarding proposals to phase out POP, IMAP, and SMTP services. POP services are the oldest of these and will probably be first to go but throttling solutions, discussed further below, are a better way to deal with concerns. Ongoing discussions should be vetted with the Computer Security Subcommittee and the ITCC. The technical issues were provided by Karl and are summarized below.

Mail Protocol Reduction

UM wants to reduce access to mail to basically just Exchange and Web connectors. This means turning off POP, IMAP and SMTP access for user clients such as Thunderbird, Eudora, etc. The major reason is to reduce the number of target ports used by spammers with compromised accounts. With every SPAM run, we run the risk of being blacklisted. While POP is a very old protocol and should go away, the other two are problematic as they are good fall backs. The down side is the spammers can still use Outlook and the Outlook Web Application (OWA) to continue to send spam. It would be better to have outbound automatic throttling/queuing that slow down a mass mailing and alert staff once a threshold is crossed. Even slowing it down or stopping it can keep us off blacklists until personnel can find the compromised account and take action.

Discussion continued with an emphasis on throttling as a preferable alternative to removing services.

Pertaining to the Faculty Senate referral, we noted that the ITCC was actually quite proactive about computer security issues. We formed a Computer Security Subcommittee a decade ago in order to provide rapid (even same day) response when required. We also have learned from the mistakes of other universities. When these hit the news, a query goes from the Computer Security Subcommittee Chair to IT as to whether we would have fallen victim to the same attack. Usually the answer is no, but whenever there's an adjustment to be made, it gets done.

More importantly, the ITCC anticipated that computer security incidents and related problems can occur despite best efforts, so we used an infamous incident (see attached article) to create a case study in how to respond to such problems, circulating it first to the Computer Security Subcommittee and then to the campus community via an ITCC Open Forum in March 2011. This resulted in the following unanimously approved motion:

The ITCC recognizes that problems are never guaranteed to be avoidable. Therefore we recommend that the university adopt a perspective of learning from problems rather than identifying scapegoats. We also recommend that individuals with responsibilities for the protection of sensitive data seek the involvement of professionals to ensure that safety is provided. Furthermore, guidance to accomplish this should be provided to people with such responsibilities. (March 2011)

This motion was brought to the Faculty Senate on June 16, 2011, where it also passed unanimously. <http://facultysenate.mst.edu/media/campussupport/facultysenate/documents/fsminutes/2011/FS.Minutes.06.16.11.pdf>

The reason for this policy is that organizations that look for scapegoats seldom learn from mistakes and waste energy assigning blame. In the case study, a university aggravated the situation rather than improving it when it responded inappropriately to a security breach. This policy is intended to protect Missouri University of Science and Technology from making the same mistake. It was very clear from discussions in both the ITCC and the Faculty Senate that this applies to Faculty and Staff.

The ITCC also dealt with the recent computer security incident in both its October and November meetings as reflected in the minutes. The November meeting resulted in the following motion:

The ITCC insists that filtering of outbound spam begin ASAP, and requests a report on this at the next meeting or sooner. (November 2012)

In partial response to this motion, Uetrecht (absent, but relayed prior and communicated at the meeting) provided a report that Cisco Ironport already existed at the time of the incident last Fall and is now being tweaked to improve filtering of outbound spam, in response to our motion. Lutzen reported that Ironport is being upgraded this weekend. Bax commented that he had been involved with Information Security for a long time, that nobody is perfect, and thus it's a learning process. Bax shared a list of requests for Computer Security Subcommittee to give feedback on. These were received yesterday and forwarded today so we will try to have some feedback for those soon. It is clear that improving distribution list management is needed for better security.

Lutzen provided list of computer security items that everybody should know, attached. We would also like to develop custom "throttling solutions". The ITCC is very supportive of the goal to create a strong in-house capability to develop this class of solutions, which focuses increasing levels of attention (up to full blocking) on excessive volume of outbound email.

Bax also mentioned that the university business policy manual has been updated. Business policy BPM 911. More details will be covered at a future ITCC meeting. (This was also in the list provided by Karl.)

Bax mentioned possibilities of improving our computer security posture by getting students involved, tiger teams, scholarships, etc. Tauritz mentioned that the ACM Security Team is a major resource that could participate in this. He pointed out that expert Sandia visitors were astounded with how well we work with security and faculty researcher collaborations on this campus.

Motion: Computer Security is a strategic resource for this campus and a locally-based strength for the whole UM System. The current strategic planning process should consider enhancing computer security resources located at Missouri S&T to be responsive to needs of the whole system as well as supporting computer security research and data management.

Moved by Vojta, Yu 2nd

Passed unanimously

Wunsch will discuss this motion with RP&A on Monday.

Research Computing input requested

Bax requested to review redundancy requirements for high-performance computing. This needs to be revisited, so the ITCC referred it to the Research Computing Subcommittee. They have looked at this and will look into it more. Most researchers reported that they use some kind of checkpointing but they think that formal requirements aren't enforceable.

We don't have redundancy here so if code isn't checkpointed, a power loss will cause loss of the whole job. With upcoming construction this could become more of a problem.

Teaching & Learning Technology Conference and March ITCC Meeting – do we want to do the retreat then or do a full day in April or May? Discussion and decision.

Since we are meeting two weeks before classes, we aren't getting a representative set of opinions, so we decided to decide at the next meeting. IT will send us a survey: half day March?, day in April?, day in May? Two half days? We will discuss this at the February meeting.

Meeting adjourned 5:35 PM