,ITCC Minutes, October 17, 2012
4-5pm Faculty Lounge, ECE

Attending:

Frank Liu, Karl Lutzen, Richard Dawes, John Singler, Vicki Callaway, Bob Cesario, Fatih Dogan, Thomas Vojta, Matthew Richard, John Bax

CIO Search Update

> The CIO Search Committee received applications from 52 candidates. We intend to select 7-10 candidates for the first round of interviews. We will contact the candidates whom we would like to interview. The candidates who we have eliminated from consideration will receive a communications from the Committee in the coming weeks. You application remains under consideration if you do not received a communication from the Committee.

Approve last meeting's minutes

Approved (John moved, Richard second)

Plan upcoming meeting times including potential retreat

The committee decides that the ITCC regular meetings will be held at 4-5:30pm on the second wed. on each month in the Spring and Fall semester, and ITCC retreat should be held early next year, depended on the arrival of the new CIO.

October Cybersecurity Awareness Month Briefing

Two videos are submitted for this time. Since its participation is low, IT may not do it in the future.

Space Issues, Org Chart

John distributed the latest IT organization chart and the committee briefly discussed it.

Email issues

John Singler brought the issue raised by one of faculty members in his department. Below is the discussion summary.

> Over the past three weeks, our campus and the other campuses of the UM system have been the focus of increasing phishing and spamming attacks. The phishing led to the compromise of some people's mst email accounts, which led to an extremely high level of spam email issuing forth from our campus email. The level of spam was so high that *all* mst email, as well as all of UM, has been *blacklisted* by various agencies. Therefore, any email sent to an off campus email address (in approximately the past two weeks) may have be marked as junk email by the intended recipient's email program.
>
> UM IT has been forced to take emergency measures to combat the high level of spam activity (in order to remove the blacklisting from as many agencies as possible). The following restrictions have been put in place:

1. Port 587 must be used to authenticate email – smtp only with a limit of 9 email's per minute; Outlook and Outlook web app (owa.mst.edu) are not affected
2. SMTP email can have a maximum of five individual recipients – lists (such as through Google groups) only count as one recipient; Blackboard and Joe'ss email are not affected; Outlook and the Outlook web app (owa.mst.edu) can also be used for more than five recipients

The faculty was *not* notified by IT of these (emergency) changes for the following reason. Mass notification of similar email changes was made on one more other universities. The phishers obtained a copy of the notification email, modified this notification to create a new phishing email, and attempted to use this modified email to gain access to more email accounts. Therefore, our campus IT decided that a mass notification might cause more harm than good.

Our campus IT makes the following recommendations:

1. If you are not using Outlook or OWA, create and use email lists (e.g., using Google groups) in order to send emails to more than five individual recipients. Our campus IT hopes to increase the number of individual recipients allowed on each email (possibly to 15), but this may not be done immediately.
2. Strengthen passwords (even up to 12-14 characters) in order to prevent hacking and further corrupted email accounts.
3. If you sent an email in the last two weeks and expected, but did not receive, a response, then it is possible that your email did not make it to the intended recipient. You should consider resending such an email, or (gasp!) consider making a phone call.
4. Recommend that all faculty and staff use certificates (also called Digital ID) with their email. It can ensure that the recipient can verify that it was you that sent the mail. It should to be installed on all devices that a person sends mail from regularly. It also allows two parties to have unbreakable encrypted conversations for sensitive matters. More details available at, https://wiki.mst.edu/security/public/incommon_certificate_requests.