Minutes of the UWM IT Policy Committee

September 9, 2011
8:00 – 9:30 a.m.
CHA 211

The meeting was called to order at 8:00 a.m. by chair Chris Burns.

Discussion of IT Security Incident

Vice Chancellor Tom Luljak and Steve Bruckbacher reported on a security incident that resulted in notifications being sent to 75,000 individuals due to a data breach incident that may have exposed records containing confidential data. Legally, the University is only required to send notifications when it is known for certain that personal information has been accessed, which did not happen in this case. There is no evidence that either names or Social Security numbers were accessed, but the "door was left open." No stored financial data for individuals or the University is at risk. The incident was likely a search for intellectual property.

The number of return inquiries from those individuals who were notified was below expected levels. An off-site call center was set up to handle the inquiries with a secondary call center on campus. There were 170 calls to the primary center and an estimated 2/3 were escalated to the local center. The hot line to the primary call center is still active and there were three calls in the last five days.

The vast majority of the calls came within the first 10 days. Many were from elderly people who did not understand what the notice was about. In 80% of the situations, although the callers were not happy, they were satisfied. The remaining 20% of the callers were quite upset and wondered why the University would be keeping information on them for a long time. Brad Houston recommended that University departments create retention policies to ensure that un-needed information is not available to be compromised.

The initial media coverage of the incident was extensive, but after three days the number of stories fell off dramatically. Despite the best efforts to contact everyone via US Mail, hundreds of letters were returned. Letters will be resent to those for whom the Post Office has provided forwarding information.

An outside forensics firms was engaged to analyze the situation in conjunction with the departments that own and manage the compromised service.

It was recommended that there should be a privacy policy for student records that is distinct from the Security Policy. Ed Mabry recommended the compilation of recommendations based upon this incident. Internal Audit will be conducting a post-incident review that will include:

1. Identifying internal control weaknesses
2. Taking an overall look at the controls that are in place
3. Reviewing the process of the response

Legal Affairs and the State Privacy Office will be conducting presentations on campus.

Approval of the May 2011 Minutes: M/S/P

Review of 2010-2011 ITPC Annual Report

Chair Chris Burns reviewed the committee's annual Report that was submitted to the Faculty Senate during the summer.

UWM WiFi and eduroam

Melissa Woo explained that a six-month pilot is underway for a next-generation 801.11n wireless network in the core of the campus between the Union and the Library. Once someone logs in, their traffic is encrypted. Devices need to be set-up only once to use the new network.

If guests are invited to campus, UWM faculty and staff can contact the UWM Help Desk to sponsor their access to the network.

There is also a public, unencrypted wireless network that is limited to Web access and offers limited network capacity in the coffee shop area of the Learning Commons for use by guests who don't have their own panther**LINK** accounts. The public wireless network is not recommended for use by UWM faculty, staff and students.

UWM is the 18th institution to join the eduroam consortium that enables people to get wireless access at participating institutions around the world using their ePantherIDs and passwords. For example, LIGO scientist Scott Koranda was recently in the Netherlands and able to get on the Internet with his UWM credentials by using eduroam.

The wireless pilot project will continue until early January. At that point, the pilot will be evaluated, and if the service is considered appropriate for expansion, funding will be sought to extend the capabilities to the entire campus.

Faculty/staff pantherLINK Quota Increase

Melissa Woo reported that panther**LINK** email quotas for faculty and staff are being increased from 5 gigabytes to 7.5 gigabytes. The 7.5 gigabyte limit will be a hard quota. Those who are currently using more than that amount will be grandfathered in.

A limit is needed because those who use excessive amounts of storage can impact panther**LINK** performance for the thousands of other accounts on the same server. There are still panther**LINK** performance problems caused by people sending mass e-mail broadcasts during daytime hours.

Although approval has been given to automatically delete e-mail messages that have been left in Trash folders for more then 30 days, the process has not yet been implemented.

Choosing Liaisons to Other Committees

Liaisons between the IT Policy Committee and other campus groups were chosen:

- Academic Planning and Budget Committee -- Chris Burns
- Ed Tech Fee Committee -- Ed Mabry, Woonsup Choi
- Web Steering Committee -- Tracey Buss, Chiu Law
- panther**LINK** Steering Committee -- Michael Zimmer
- Tech Users Group -- Brad Houston
- Research Policy Committee -- Prasenjit Guptasarma will be invited to serve
- Mobile Steering Committee -- Ethan Munson