Information Technology Committee
Minutes
2006-2007 Meeting #6
March 28, 2007, 10:30 – 11:30 a.m. (Pacific Time)

Present: Anderson (Chair), Cronk, Frenzel, Funabiki, Goodwin, Hughett, Krogh, Merrell, Schlater
Absent: Pendegraft
Guests: Tony Opheim (ITS)

Call to Order: Chair Anderson called the meeting to order at 10:30 a.m. in room 101 of the Ag Biotech Building

Business:

1) IT Security
   Tony Opheim, Chief Technology Officer from ITS, participated in the meeting to share more information and insights into the ongoing effort to identify and resolve IT security issues. Tony discussed how ITS has been working with the UI Office of General Counsel to examine legal issues related to obtaining and retaining sensitive personal information such as social security numbers.

   Tony also provided some details regarding the university’s latest IT-related security breach at the Institutional Research office. It appeared that the person(s) at fault was (were) unaware that the files they had placed on a public server contained sensitive personal information. Harvey Hughett said the incident once again illustrated the need for better user education.

   Tony described steps ITS was taking to reduce user access to personal information. The committee discussed the need to communicate the changes to the university community, particularly to those who will be directly affected by the changes.

   Tony also reviewed the process ITS was using to audit computer and server systems across the university. There are now more than 2000 servers online at the Moscow campus. Approximately 90% of those machines are networked printers or multifunction devices. These networked devices present new challenges because most users are unaware of their potential vulnerabilities.

   Jim Frenzel asked whether ITS had considered using “dumb” terminals or thin client systems to handle sensitive information. Tony said such client/server technology could help solve some but not all of the security problems. Even if thin clients were implemented for some services, they could not supplant the need for PCs in most offices.

   Tony said that, at the present time, ITS was focusing on identifying risks rather than developing new security policies.

   The committee discussed other security-related issues including the possibility that other personal data, such as mailing addresses, might be considered protected information in the future. That development could have a significant impact on some university activities such as fund raising. Harvey commented that the recent security breaches already had made some potential donors very nervous about their relationship with the university.

2) Other Discussion Topics
   During the short amount of time that remained, Peter Goodwin asked Tony Opheim whether users were at risk when they accessed personal information over a wireless network (e.g., while
traveling). Tony’s answer was “Yes, the data can be at risk.” Tony added that the Banner encryption level would help reduce the vulnerability. He also advised that a wired connection (e.g., sometimes available in a hotel room) was not necessarily any more secure than a wireless connection. He recommended the use of a Virtual Private Network client for remote access.

**Adjournment:** The meeting was adjourned at 11:30 a.m. The next meeting will be held on April 25, 2007 at 10:30 a.m.

Respectfully submitted,
Professor Erik T. Anderson, Chair 2006-2007