

IT Managers Meeting

October 7, 2009

Pre-mtg Vendor: 12:15 - 12:50 pm -- Sophos - slides

Regular meeting: 1:00 - 2:30 pm

[Meeting Slides](#)

I. IT Updates

Information Security Awareness Day - October 29, 2009

The 2nd annual campus ISA Day will be in the Union Ballrooms. There will be presentations on subjects for every campus member; see <http://www.secureit.utah.edu/isad/agenda.html> for details. Please encourage your end-users to attend. We will be giving away free McAfee anti-virus to students and SmartDraw to staff. There will be refreshments and several chances to win iPods and Adobe Creative Suite 4 - a Windows and a Mac version. We are also doing an IT Managers workshop on Qualys scanning reports in conjunction with the event. It will be held at 10:00 am in Union Room 312. If possible, please post an ISA Day poster in your area to help us get the word out: http://www.secureit.utah.edu/pdf/isad/isaday_poster.pdf. Thanks!

AT&T/NextG Cellular Coverage Project

The project is progressing. NextG said yesterday that they were pulling in the last piece of fiber and doing the splicing and hope to complete that by the end of this week. Programming and testing will then begin and will take at least two weeks. The last week of October they will perform the final commissioning of the network and by the end of the week have it ready for public use. During the testing, they will be testing in-building coverage with the targeted areas in mind. Once the system is on network we will continue to do in-building coverage testing and see if additional tweaks are required.

Firewall Change Process:

This won't affect your department firewalls, will affect hospital firewalls and the campus front door. Go to <http://orderit.utah.edu> and choose the firewall option -> Start Here-> login to ULogin. Changes needed to be submitted by Monday midnight; NOC will meet with ISPO and ISO each Tuesday and firewall changes will be done each week on Tuesday night from 7 - 8 pm (they can also do them on Wed & Thurs in that same time frame if there is a problem with what is done on Tues).

Wireless Update - Brent Elieson - [see slides](#)

Project is to get to wireless ubiquity. Single IP pool and routing is one of the criteria. UConnect will be routed off a single wireless node - mobile device IPs won't change as it roams. UGuest routing is being moved to wireless node. AP Rollout - 15 minutes per AP is estimated. Please sign up with Brent after this meeting (or contact him directly). A timeline for the rollout into 2nd quarter 2010 is on the slides.

II. ISO block: - Dave Feyler - [see slides](#)

Scanning results are being trended and broken down by department to help everyone. Thanks to everyone's efforts in reducing vulnerabilities - gains have been made but we need to do more! Focus on encryption- Get off DES and WEP - known to be easily cracked. Think about Nelson's recent email about WEP. - Good crypto systems: Triple DES and AES (which is NIST approved). If nothing else, use a Zip file with AES 128 or 256. - Protocols: Telnet and FTP are

not secure. SSH, SSL, ___ are secure. - PHI in UMail emails' subject line encrypts the email-encrypted password manager (KeyPass was mentioned) to help deal with all the passwords

III. IT Highlight: Trevor Long, College of Ed - [see slides](#)

The College of Education tried to offer free printing to students for a time but began to see instructors from other colleges coming over to print tests, etc. They are moving to UCard printing at the semester break. Probably their best purchase to date was an IP KVM. They adopted OCS (inventory & package management) and Team Viewer (remote desktop) after hearing that CSBS (Demian) is using them. (wiki: doing docuwiki) They're very happy to be using UMail now; it saves them a lot of time. They also have a child domain in A.D. FTPES allows their faculty to access files remotely - maps them right to their user files (they have to use Filezilla with it) - it's integrated with the A.D. They've been using Splunk to aggregate login information for SCAC funding (required). (Richard Glaser says Keyserver does that, too.) They send about 400 GB offsite for backup with PSI every week. PSI only charges you for the cost of the tape (and they only insure the cost of the media) - they're not very expensive. CoE rolled back to 32 bit for print services, but they use 64 bit for other services. They're also very happy with the campus VMWare licensing.

IV. HITEC Regulation and Information Security Policy - Chris Kidd - [see slides](#)

PHI: Protected Health Information (The HIPAA Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)".) Breach notification: the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of it (a HIPAA violation). If it meets the harm thresholds, it has to be reported. The patient or affected individual must be notified as soon as possible within a 60 day window. It is not acceptable to wait until the 59th day to start. Notification must happen as soon as possible if the incident meets the notification criteria. If it affects 500 or more people, HHS and the media must be notified. Fines have increased dramatically for willful acts. Call the Help Desk w/in 24 hours after a breach occurs! The new Info Security Policy is going out for feedback - please give us some. The PHI Rule will be attached to the new (revised) policy. The plan is that the current policy 4-004 will not exist in its current form once the new policy is approved. A data classification rule is also about to go through the approval process. 3 categories: restricted data, sensitive data, public data. This will give examples and make it more clear for IT Managers. Chris will post the draft policy for feedback. Chris will send something out that's based on the data classification within the week. We want your feedback on it too (especially if it's not clear).

V. Laptop encryption discussion: What Works, What Doesn't - panel discussion

a. EndPoint/SafeBoot - Kyle Hansen, IT Service Automation - [see slides](#).

Kyle isn't trying to sell EndPoint. Early 2008 ITS did a "bake-off" and McAfee SafeBoot (now EndPoint) won. It:

- Is NIST approved,
- Has centralized management and control ,
- Was competitive in cost (\$42/year 1, \$31/years 2 & 3)
- Has proof of encryption
- Only supports Windows currently, they are working on a Mac solution They have done 835 laptops. They got the desired results and they've had a very low failure rate - only 3 laptops that had older hardware had problems. Only 13 tickets with real problems

(machine had to be reimaged). They will be looking at other products in the next 6-8 months

b. PGP Desktop - Steve Jeffs, CSBS - [see slides](#)

- Used PGP Netshare for terminal server- client based. Folder is automatically locked at logout. Downside: the folder is decrypted when it's unlocked. User education for temp files and working folders to stay encrypted. Upside: The PGP Zip wizard prompts to shred the unencrypted version of the file.

c. Apple-- Richard Glaser - [see slides](#)

Richard provided quite a few screen shots showing how to use both Apple options.

- Disk Utility
- FileVault - built-in since Mac OS 10.3 or later

d. TrueCrypt - Dan Hutten

They hand out encrypted thumb drives in Pathology ... more on this and the whole encryption theme to come.