Information Security and Compliance Committee

Meeting Minutes

University Hall, Room 310

January 18, 2018

Present: Megan Pfaltzgraff, Jane Combs, Cindy Lusby, Elizabeth Aumann, Lorre Ratley, Tina Bosworth, Rick Grant, Eira Tansey, David Baker, Jesse Fatherree, Tamie Grunow, Kyle Hern, Bo Vykhovanyuk, EdDadosky, Todd Beekley, Tara Wood, Michael Miller

Guests: Geoff Costa, Tyler Hopperton

Apologies: Bruce Burton, Matt Williams, Brett Harnett, Mark Stockman, Dianne Brueggemann, Mel Sweet

New Business

1. Welcome and Overview
2. Review of November Meeting Minutes
   o Todd Beekley moved to approve the minutes; Elizabeth Aumann seconded the motion. The motion was unanimously approved.
3. European Union General Data Protection Regulation (GDPR) (see attached handout)
   o GDPR was adopted by the EU in April 2016, it will be effective May 2018. This will replace the EU data protection directive of 1995.
   o GDPR protects the Personal information of all natural persons physically within the EU ("EU data subjects").
   o UC is in the process of adding GDPR coverage to its cyber insurance.
4. OnBase – Purging Data
   o OnBase is UC’s scanning solution used by several departments across the University. There is a need for automated capability to purge scanned documents in accordance with University retention schedules.
   o Additional OnBase modules are available for purchase from Hyland (the parent company). These modules allow the data owners to run reports about stored data and
identify images appropriate for purging. A meeting is scheduled later this week to review the costs, scope of the project and to determine if this will move forward.

5. DUO Update
   o The Duo Access Gateway project has been going on for the last year. July 31st was the initial start to the pilot testing Duo on UCFlex with the Controller’s office, HR, OIS, and BCS. During the month of September, phase two began which opened it up to business users with a 2 month opt-in period. During the opt-in period, 70% of users enrolled. As of November 1st it was mandatory enrollment for all business users (1,414 users are currently in mandatory enrollment). On January 8th there was an email sent to all other users in UCFlex encouraging them to use the Duo mobile app, which is an industry standard. Approximately 600 of those users have enrolled since January 8th. The plan is to go live on March 1st. This will require all UCFlex users to use Duo with no one allowed to opt-out. There are options for people who don’t have landlines or cellphones.
   o If passwords are comprised, with Duo users are still safe. Users are more responsible for a breach when they share their credential now that UC is using Duo. Duo offers reasonable control. Compromised student accounts is an issue. OIS plans to work with Student Government to implement Duo on Office 365.
   o The Help Desk has been a part of the project from the very beginning. Geoff Costa has been working with UCIT PIO to address communications to users. There have been very few issues—mostly about how to setup their device. There is a website and KB articles for assistance. 24/7 availability for emergencies via a dedicated line; Emergency is defined same for Duo as for UC Helpdesk. IT made changes to the load balancing systems, so they now have redundancy for Duo. In the event of a shutdown, service will transfer to SOCC.

6. Trickbot Malware
   o On December 20th, Office of Information Security received notifications from some users that their computers were behaving strangely. They found that the machines were infected with a malware worm (worms spread automatically across networks). UC’s virus was let in via a phishing email and spread through regular file sharing. A little over 3000 machines have been infected and they have cleaned up a majority of the machines now. When UC was hit with the worm, it was only 3 to 4 days old throughout the world so McAfee didn’t have protection for this malware, but they quickly created it.
   o The official name is Trickbot and its goal is to steal banking information. It impersonates banking sites and copies the SSL lock. The version at UC was mining crypto currency. Within the first 2 hours of notifications, OIS was able to block it. McAfee was able to remove it, but not all systems on campus are a part of McAfee EPO. Up to 1,500 machines may still have infected files.
   o OIS has been communicating recommendations via IT Managers and other methods encouraging users to join McAfee EPO and providing recommendations for how to slow or stop the spread of the virus.
   o OIS is working to resolve the issue daily. Though it is contained, it may be around on our network up to a year or so. Out of the 3000 machines infected most have been blocked
from communication on the network so it cannot spread. Noticeable symptoms of malware are lock up of computer because virus uses all resources. Trickbot primarily hit Windows 7.

7. **Network and Phone Refresh**
   - The Board of Trustees have approved the $23 million infrastructure upgrade. This will be a 24 month (tentative) project. This will impact the entire UC campus. All new edge switches will be installed, phones will be upgraded to VOIP (PBX is 20+ years old), and all wireless routers will be replaced. That translates to 12,000 network switches, 8,000 phones and 4,800 wireless access points, all from Cisco. UPS (Uninterrupted Power Supplies) will be installed in all closets. The network switches need to be replaced before the VOIP phones can be installed. There is plan to start on phones in late spring staggered with network switch updates.
     - Note: The 4800 wireless access points will be updated to support 802.C for higher bandwidth and throughput. The new switches will have 1 GB to the desktop with POE (power over Ethernet).
   - The network hardware has been purchased, received, and is being configured. The first building upgraded will kick-off in February at HPB/Kowalewski, then the CCM node will be next.
   - Official announcements will start in late January. The schedule and notices will be sent out three (3) weeks in advance of the upgrade to specific locations to inform building managers and faculty of the upgrades. Upgrades will start at 4AM and finish by 8AM to minimize impact to classes and business. UCIT will have a website with work schedule posted soon.
   - Upgrade of network switches will be completed in December 2018. Other upgrades will run in parallel but will be staggered. Phones are being converted to VOIP and receive power from network switches. Wireless and phone upgrades expect to be complete within two years.
   - NOC is working with P+D+C to update all network closets, HVAC, and electrical upgrades to accommodate new uninterruptable power source (UPS). UPS will be transitional power for generator switchover for monthly tests.
   - UC Reading (old GRI), UCRI and Victory Parkway will have full upgrades. UCCC will have their phone system upgraded. UCBA will not be included in this project.
   - There will be additional segmentation of the network with this project which will offer better protection from Trickbot malware type viruses.

8. **Miscellaneous**
   - **FISMA Update**
     - Received feedback from Office of Research and will be doing a pilot in late February with researcher from College of Engineering.
     - Bo will send an update to the FISMA task force.

9. **Adjourn**
   - Meeting adjourned @ 11:25 AM.