



Committee Co-Chair

Bo Vukhovanyuk

AVP, UCIT

vykhovbn@ucmail.uc.edu

(513) 556-0803

Committee Co-Chair

Lorren Ratley

Dir., Privacy

ratleyln@ucmail.uc.edu

(513) 558-2733

Information Security and Compliance Committee

Meeting Minutes

University Hall, Room 420B

August 18th, 2016

Present: Bo Vukhovanyuk, Eira Tansey, Diane Brueggemann, Cindy Lusby, Katrina Biscay, David Baker, Jesse Fatherree, Lorre Ratley, Matt Williams, Ed Dadosky

Apologies: Angela Sklenka, Gary Grafe, Jane Combs, Brett Harnett, Mark Stockman, Mel Sweet, Tara Wood, Tina Bosworth, Bruce Burton, M.B. Reilly, Kyle Hern, Tony Iacobelli

New Business

- Welcome and Overview
- **Review of July Meeting Minutes**
 - Need to update membership on minutes and agendas. Remove Dan Beerck, Amanda Bill, Alla Lobkis, add Kyle Hern
 - Bo will follow up with BCS to see if they have a member to replace Gary since his role has changed
 - Lorre Ratley moved to accept the minutes; Jesse Fatherree seconded the motion. The committee voted unanimously to accept the minutes.
- **HIPAA Policy Update – Lorre Ratley**
 - Changes to units covered
 - OGC is seeking another legal opinion to determine covered entities
 - College of Medicine may not be a covered entity but all data will still be protected
 - Hoxworth is not a covered entity, but is a business associate
 - Policy written as if whole university is covered but that is not true – policy will be rewritten more succinctly and reference OIS security policies.
 - Lorre will provide timeline for rewrite at a later date.

[Current Membership](#)

- UC Health staff should not be downloading data containing ePHI to UC systems.
- **Policy Status Update – Matt Williams**
 - Data Governance Classification Policy was approved by this committee and it move to IT Council
 - See attached for policy statuses.
 - HIPAA Info Sec policy will be retired when Office of General Counsel HIPAA policy is finalized and approved
 - Newest versions of policies are updated and available on SharePoint site
 - Computer locking policy was retired.
 - Incident Management Response was changed to Information Security Incident Management Response policy
 - Nelson is presenting last 4 policies listed to Council of Deans today
 - Other policies in early development and will be shared in the future if they become policy
 - Perimeter Firewall policy, which will be renamed if it becomes policy
 - Elevated Access Policy – was an IT specific policy
 - Comparing and contrasting policies with other comparable institutions and Ivy League schools.
- **Other Items**
 - **Data Loss Prevention (DLP) – Katrina Biscay**
 - Code Green Box integration is working and have received positive feedback from university community
 - UCIT – PIO is communicating new functionality and is in KB articles
 - Conducted overall scan of data in Box and no restricted data is there
 - Will continue to monitor with weekly scans and dynamic scan with each file upload
 - Primary goal is to prevent accidental exposure of data
 - **Katrina will send Jesse the PowerPoint presentation being shared with key IT staff**
 - Box will remove restricted files but breadcrumb will be placed on device to show where file is in restricted file on Box.
 - For DLP prevention education for users send them to kb.uc.edu and search for Box
 - **Phishing Issues – Katrina Biscay**
 - Last 3 weeks have seen significant increase in attacks (12k+ attacks)
 - Graphics, logos, and language are correct in latest messages, which makes them look authentic
 - Attacks are very sophisticated and include email hacks with rules to remove account notifications
 - Attacks originated in Nigeria
 - Had 183 compromised accounts but no damage done to UC systems
 - Other universities experiencing increased attacks as well but they have experienced damage (stolen paychecks)
 - UC has controls in place to protect direct deposit accounts for paychecks
 - SPLUNK detected attack at UC and enabled OIS to notify Payroll within 20 minutes

- Additional controls will be added in the future
 - User education will increase
 - Notification of users who have been compromised – currently accounts are immediately disabled without notification
- Mobile devices render emails differently and make everyone vulnerable to accidentally clicking a link
- OIS requests everyone to forward phishing email to them abuse@uc.edu
- **Creating a better definition of research data**
 - Scholar.uc.edu is institutional repository for intellectual output
 - People can put data in repository and keep it private for self only, or share with specific collaborators, or make data public
 - Informationist (Librarians) work with faculty to help them understand issues related to data management
 - Eira suggests Ted Baldwin or another Informationist attend a future IS&CC
 - **Eira will follow up with Lorre to workout logistics of inviting someone**
 - In future, UC Data Governance committee will be formed.

Adjourn

Committee adjourned at 11:08 AM.

[SharePoint Site for shared documents](#)