IT@UC GOVERNANCE

Information Security & Compliance
IT@UC
University of Cincinnati
PO Box 210658
Cincinnati, Ohio 45221-0658
Suite 400, University Hall
51 Goodman Drive
(513) 558-4732

Information Security and Compliance Committee
Meeting Minutes
University Hall, Room 420B
February 18th, 2016

Present: Bo Vykhovanyuk, Alla Lobkis, Brett Harnett, Lorre Ratley, Karen Kovach, Todd Beekley, Jesse Fatherree, Jason Green, Matt Williams, Angie Sklenka, Tina Bosworth, Eira Tansey, Neil Holsing, Katrina Biscayne, Cincy Lusby, David Baker, Mel Sweet

Apologies: Bala Ramachandran, Jeff Corcoran, Gary Grafe, Bruce Burton, Mark Stockman, Tara Wood

New Business

- **Welcome and Overview**
  - Welcome New Graduate Student Rep, Bala Ramachandran (not present today)
  - Introductions
- **Review of January Meeting Minutes**
  - Three changes were made to the minutes
  - Once minutes were updated, the committee unanimously approved them.
- Review of Action Items
  - Bo Vykhovanyuk, Lorre Ratley, and a representative for Eira Tansey met to discuss retention issues. They will meet again and bring recommendations to the committee next month.
  - Jane Combs met with Tara Wood regarding Export Controls and the Research Directory ***Completed***
  - Tara Wood attended IT Managers February meeting and has other governance meetings scheduled in the future. ***Completed***
- **Incident Response Update**
  - OIS is working on outlining the high-level policy, which includes a procedure.
  - Procedure was based on UC Berkeley template.
  - The draft policy Includes incident guidelines, who to contact in case of an incident, including Office of General Council
  - An incident has a wide scope, and is defined as any issue that includes UC data.
  - OIS performed a tabletop exercise with Enterprise Risk Management regarding incident response.

UNIVERSITY OF Cincinnati

- OIS has received feedback from key stakeholders and it has been incorporated into the policy.
- In the March meeting, this policy along with others will be brought to the committee for review.
- Policy and procedure should be available on SharePoint in next few days to allow committee members ample time to review and comment before March meeting.

- Data Loss Prevention (DLP)
  - Conducted proof of concept; only two (2) vendors met requirements.
    - Selected Code Green. It was approved by IT@UC leadership team and is now in Purchasing
    - Code Green met all requirements; meeting all requirements is a rare event.
    - Thanks to CoM staff, and Lorre Ratley for assistance with proof of concept
    - OIS hopes to start staged rollout by April 2016
    - Will include Box integration
    - Funding is for next 18 months, need to think about renewal funding.
    - Network traffic includes email scanning.
    - Code Green fingerprints all valid sensitive data, which reduces false positives.
    - Iron Port (our current tool) has detection and encryption components; OIS will stop using detection component when Code Green is rolled out.
    - Code Green helped identify sensitive data flowing from UC Health that was unencrypted; data has now been encrypted.
    - Will allow for future planning for handing restricted data.
    - Box allows syncing data with personal devices; Code Green removes that ability.
    - Can also notify when sensitive data has been transferred and will move it out of personal device and put it back into secure location.
    - Each department can customize Code Green installation to meet their specific needs.
    - OIS will help departments determine what data needs to be protected.
    - Code green can identify situation when multiple non-restricted data pieces are presented together to create a restricted data scenario (e.g. last four of SS# and are not considered restricted data but it would be if presented with other identifiers)
    - Has 5 appliances with unlimited VMs.
    - Code Green will allow CoM to use individual Box accounts instead of admin accounts.
    - Can setup rules by group.
    - Neil Holsing would like to have a test group for CoM before it is fully implemented.
      - OIS will work with Jesse Fatherree to create a test group
      - Can pilot it on a few accounts now if desired
      - Have meeting scheduled with CoM in early March to develop plan.
    - Need to develop good communication plan around Code Green.
    - Need to develop a plan specifically for medical records.
    - Plan to have Code Green fully working to scan Box files by end of fiscal year
- **Single Sign On / Identity Management**
  - Single sign on issue is driven in part by students.
  - Once turned on, single sign on works across all applications except UCFlex, which causes some risk
    - OIS is working with HR to implement single sign on for UCFlex.
  - In corporate environment risk is mitigated by having one policy for customers and one for employees
  - In higher-ed all are using same policy.

- OIS plans to speed up roll out of multi-factor authentication process to address risk issues.
- Nelson Vincent is meeting with Catalyst team soon to discuss risk mitigation plans.
- OIS recommends using Shibboleth, but the final decision is up to the application owners.

- **External Penetration Testing**
  - OIS engaged a third party company to perform external penetration testing.
  - All public facing system tests are scheduled 3/21 – 3/24 during spring break to minimize impact on students.
  - IT admins will be notified with details as time approaches.
  - Once test is completed, takes about 2 weeks to a month to obtain results.
  - IT admins will be notified if they have public facing systems that fail the penetration tests.

- **Next Meeting:** Enterprise Risk Management presentation.

Adjourn

Committee adjourned at 11:00 am.

SharePoint Site for shared documents