Information Technology Committee
Monday, February 8, 2016
4:00-5:00
Mrak Hall, Room 410

Agenda

Present Members: Matt Bishop (Chair), Giacomo Bonanno, James Fadel, Michael Kleeman, Jeremy Lea (AF Rep)
Absent (excused): Vladimir Yarov-Yarovoy

I. Faculty Response to Cybersecurity Training
   a. Complaints include that it was not targeted appropriately for the university. Different levels of difficulty should have been offered for this training.
      i. If there were different levels, it would be difficult to identify who should take which training.
   b. A general letter should be sent regarding the adequacy and necessity of all training (the cybersecurity training will not be the only point). This letter should address whether faculty time is being spent in useful ways when they take these sorts of trainings.

II. New LMS Implementation Update
    a. Will be discussed at March 16th meeting by David Levin

III. BigFix – Will be mandatory
   a. Consequences for not complying?
      i. Not yet established
   b. There is an exception process, with exceptions to be signed by chair and dean (e.g. if the software cannot run on certain hardware).
   c. Some departments already have their own Chair and IT committee, so exceptions would be done through the department rather than individual faculty. Documentation is important so that IET is aware of exceptions.
   d. Trust has been lost, which makes adoption rate low.
i. A formal policy on what can and cannot be done should be created in order to build trust with the faculty. Showing people the advantage of using Bigfix instead of making it mandatory may make people more likely to adopt.*

e. André and the Provost met regarding this issue. The faculty needs language to understand that consultation has occurred.

f. A list of what is being managed will let people know what they need to manage on their own.

i. There is no central management, but it could occur without faculty consultation.

g. The Provost, CIO, Deans, and André together made the decision that this would be mandatory. With the current exception policy, the mandatory nature does not look good.

IV. Campus Monitoring from UCOP†‡

a. UCOP installed a monitoring box and people got concerned about what it was monitoring, and questions were not being answered. CIO was confronted about lack of consultation.

i. Monitoring only looks at headers and only at emails going in and out of university, not within university. It looked for known attacking sites and for patterns that indicate attacks.

b. Problem was lack of consultation and secretiveness.

c. UCOP made a decision, after the monitoring had begun which was made by attorneys. Attorney-client privilege should regard the attack and not the monitoring. (The Cyber-security Responsible Executive and a Cyberrisk committee with campus representation was put together after monitoring was already put into place). Our provost is Davis’ representation on this committee.

d. Our campus has not had any secrets regarding running Tipping Point and what gets viewed and blocked.
e. The Electronic Communications Policy has rules for campus monitoring. Does not include procedure.

V. Other Business

VI. Committee Meetings

*Formal Policy for BigFix. Michael will draft policy.
†Letter to Administration regarding openness and consultation on monitoring campuses and requiring software. Matt will draft letter.
‡We will talk to André about sending an email out to all faculty (with history and background) regarding meeting with Systemwide CIO.