Boston University Information Services & Technology
111 Cummington Street
Boston, Massachusetts 02215
www.bu.edu/tech

Information Security & Business Continuity Governance Committee Meeting

Thursday, February 7, 2013

Location: Metcalf Trustee Kenmore Conference Room, 1 Silber Way, 9th Floor

Time: 8:30am-10:00am

Chairs: Bill Long & Christie Talley

Support: Quinn Shamblin

Committee Members: Ana Bustin, Cynthia Butler Loud, Ran Canetti, Eric Jacobsen, Tracy Schroeder, Daniel Wieland, Rebecca Ginzburg

Recorder: Eric Jacobsen

Minutes:

Strategic Planning Draft Goals (Quinn)

The goal is to define action items that the University can support and give direction to IS&T. Numbered items are the actual strategy statements, with the bulleted items supporting the strategy. Despite being numbered, they are not currently prioritized.

- People will assume that the solution provided meets the requirements and unless they come with clear instructions they will not get done.
- Can the committee help us identify gaps in provided solutions?
- Coming up with an easy way to secure e-mail transactions
- Different levels of security for different types of applications.
    - Follow on discussion about "zone" versus "zone".
    - Recommend review of the Data Protection Guides.
- Presumption is that research data is open, except for Human Subject data.
- We need to focus on awareness because people are not thinking about data security during their daily tasks.
    - The less we can make it necessary to think about security, the better off we are. The defaults should all be "okay".
- We should be looking at, if anyone knows that they have access to ePHI, PCI, SSNs without a systematic protection mechanism.
- Education should go beyond our standards and policies. We need to provide a broad base education to everyone

- Leveraging ISAW for communication. Produce guidelines for the most popular (web)sites out there, e.g. dropbox, to increase broadbased understanding of risks to data, whether it's personal or not.
- We're missing "outreach" – provision of information should not be just a passive act. Administrative and academic partnerships to have them help educate the community.
- What is our baseline requirement to educate students? Explanations of risks of being online to student population. Small or no risk to institution but there may be a mission related driver to do so.
- SMG retooling curriculum, and incorporating ethics into coursework. Could try to do something similar with CS curriculum. Leverage faculty working together.
- Leverage DoS, perhaps through coffee & conversation, to get to students.
    - Online course?
    - Possible inclusion in orientation?
- Work to forge partnerships with academic units involved in security research and use their expertise to engage community
- Potential tension between seamless/embedded and not being transparent in what we are doing. Include appropriate disclosures.
- Reorganization for structure into guiding principle, then the how: technical and training (and then room for growth)
- Need to focus a bit more on business continuity. System resiliency, backups, and disaster readiness. Departments are seeking this guidance.
- Include risk of server sprawl and geographic/network spread
- Securing records by digitizing them (better than paper). : It's cheaper too.
- Need to incorporate student role into security principles.
- Additional comments on ROI point, rigorous certifications.

Proposed annual agenda draft

- Meeting Frequency Discussion / Overall Agenda
- Consider making meetings in September in the second half of September due to heavy load of the start of school.
- Consider May meeting during study period?
- University Data Retention policy covers paper and electronic. Policy is currently under the ownership of Peter Fiedler. This is something we may want to take up.
- The annual general agenda list is adopted. See the meeting materials folder.