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

BOSTON
UNIVERSITY

Information Security & Business Continuity Governance Committee Meeting

Thursday, January 10, 2013

Location: Mechanical Engineering Department**,** 110 Cummington, Room 245

Time: 8:30am-10:00am

Chairs: Bill Long & Christie Talley

Support: Quinn Shamblin

Attendees: Ana Bustin, Cynthia Butler Loud, Maria Canellos, Ran Canetti, Greg DeFronzo, John Imbergamo, Eric Jacobsen, Susan Mankiewicz, Justin Ren, Tom Robbins, Tracy Schroeder, Ari Trachtenberg, Daniel Wieland, Tanya Zlateva, Rebekah Ginzburg

Other Invitees: Reg Lo, Robert Sparks

Recorder: Deneena Lewis

Agenda

Strategic Planning – Discussion Group Input and Goals (Reg Lo)
See Presentation

- How can we get better attendance at strategy input sessions
    - If we're going to get a large number of people (t least one from each area), we would need to get requests from the department heads.
    - The time of the year may make an impact on attendance as well as availability. The shorter the time slot, the more likely sessions at the end of the day.
- IS security is always going to be sensitive.
- The shadow systems came about because the current system does not meet the needs of the organization.
- It will always be a combination of internal and cloud based services.

- We need to realize people want to use what's convenience.
- We need to know how to respond to the fact that consumer services have connections and services that we cannot replicate and if we did, people want to use the services that currently exist.
- It's important to educate the users. People should be allowed to use services like Facebook, etc., however they should be aware of the risks of using such resources.
- We're working with the project management group to provide information security questionnaires and empower them to build security into their solutions at design phase.
- People are concerned about safety on the road and what could go wrong.
- The research shows that it is hard to educate people. E-mail is an unlikely source of education.
- If we would focus on high risk areas on data security, we may be able to accomplish that section of the task.
- While it is common wisdom that security and convenience operate on a mutually-exclusive continuum. It doesn't always have to be that way. Technology exists to make things easier *and* more secure
- Security limits access for people who should not be given access. It should not unduly impede people who should have access.
- People forget that security considerations are not just confidentiality. Availability and integrity are also important components.
- We have recently moved to a new certificate provider. We can have as many certificates as we want and it won't change our cost structure
- We can enable federated login to other institutions' resources through InCommon. This is another area where there are no cost impacts. There is effort in this but not additional costs.
- We're working on an integrated system that can encrypt sensitive information automatically.
- BU has a solution for encrypting email. The capability has existed for years but the message hasn't gotten out there.
- Anyone on the BU domain can get a Data Motion and Secure Mail account free. You would receive a URL to create and encrypt the account and it's is a cloud service offering but it is encrypted.
- The proposed NAC is an enabler of greater BYOD capabilities.
- The best thing to do is open the flood gates and allow faculty to try things out and innovate, see what works.

- Part of security is figuring out how to allow as much freedom as possible to the institution. Thinking about faculty instead of administrators.
- We're working towards being able to differentiate what is more important to the community.
- Our focus should be helping people understand when they should send e-mail with a secure option.
- When using a cloud service there is a longer delay time on accountability that could pose a problem with Microsoft 365.
- Faculty members are using these cloud services despite the risks.
- There are central services that can be taken advantage of but that doesn't mean you'll have a key role in what is should look like. IT partners are directly involved in the planning process and know what their people need.
- There is a danger in over centralization. There are different missions. There may be a benefit to the distributed approach. If we have everything under "One IT".
- We need keep stakeholders involved in the process.
- The teaching technology should be particularly great. That could include support for innovation of technology.
- We need to be as open as we can in order to allow innovation as safely as possible.
- We don't want to standardize this environment.
- Communication Collaboration could be a differentiator with other institutions.

Further Discussion

- Update on PCI Compliance (February's Meeting)
- Annual Schedule (February February's Meeting)
- We will arrange a follow-up session