Committee Name: Information Security and Privacy Risk Council

Date of Meeting, Time, Location: 11/29/2011, 10AM-12PM, Poplars 017, Video Bridge 223739

Attendees in person: Merri Beth Lavagnino (Co-Chair), Eric Cosens, Dan Rives, Mary Frances McCourt, Jonny Sweeny (guest), Joan Hagen, Jim Thomas (guest)

Attendees via video: Marsha Gonzales, Kim Milford, Doug Wasitis,

Attendees via audio: Tom Davis (Chair),

Absent: Jeff Lambright, Joe Scodro, Philip Cochran, Jim Kennedy, Jill Schunk, Mike Gardner, Chris Viers, Scott Wilson, Sherrie Denney

---

**Agenda/Discussion**

**Call to Order and Approval of Minutes (5 minutes):**
Meeting was called to order and prior meeting minutes were approved as submitted.

**Old Business and New Business (10 minutes):**
- Domains 1 to 4 have been reviewed and gaps prioritized.
- Our plan is to work through all 12 domains by end of December.
- At our next meeting in January we will start a different kind of agenda with more focus on setting priorities, projects, and strategic activities.
- Domains 5, 6, and 7 - Review and Prioritization of Gaps (30 minutes)
  - Reformatted Domain 5 with chart of 3 types of people (i.e. Employees, Affiliated/partner Organizations, and Third Party Vendors) per feedback from last meeting. Rives commented that these categories will help us immensely in identifying risks by group. We will continue to add/edit these 3 domains (5-7) based on feedback from prior mtgs. Lavagnino called for any other feedback/comments on these domains. McCourt observed that we can do a snapshot/inventory, but that a change management process is vital to keeping safeguards up-to-date. How do we manage change? Lavagnino noted that there is a change management section Domain 9. Davis differentiated between change management practices in Domain 9, which are system specific, and what McCourt seems to be referring to, which is asset change management. Hagen highlighted the need for tools to help folks implement/comply w/policies (i.e. things like checklists, etc.). Lavagnino made final call for other suggestions on these 3 domains.
  - Domain Gap prioritization exercise – council members paired up to discuss the domain gaps they identified and to rank the top 3 gaps for these domains. The results were turned in and will be compiled. The gaps list will be ongoing, and exercises like this will help us prioritize our work to address the gaps.
- Domain 8 Overview - Identity and Access Control (20 minutes) - Lavagnino
  - See [https://protect.iu.edu/privacy/program/safeguards/8](https://protect.iu.edu/privacy/program/safeguards/8)
  - Lavagnino walked the council through an overview of this domain by section. This is a key activity to protect information.
Many of these efforts are coordinated by UITS Identity and Access Management unit currently managed by Jacob Farmer (formerly Alan Walsh).

Cosens gave an update on the activity of Mobile Security Committee’s activities. This committee received its charter in late October. The charter objectives were shared with the council and it is expected that the committee will produce a report of recommended actions by the end of the year. The Columbia university mobile security email and its requirements including completion of a mobile use agreement, device pins, device wiping after x number of invalid login attempts, and commitment to report lost/stolen devices to the university (including personally owned devices) was shared with the council. Cosens called for the thoughts of the Risk Council relative to the perception of the risk of mobile devices, and on the Columbia-type of approach. McCourt – culture is one thing, but sometimes we need to step back and ask ourselves where we have to be. It may be a difficult message, but one that is needed. Gonzales said that the timing is good to roll out something like this at IUPUI due to a recent breach that occurred on that campus and also asked if the committee has come up with a communication plan. Cosens – the work of the committee is farther upstream/more preliminary than a communication plan would be. Although the committee could well recommend such a plan, it will probably be left to the implementation details. A communication plan would be a next step after deciding on a course of action. Can we require this for personal devices? Council was pretty comfortable with this as a condition of accessing university information. Rives likes the idea of separating information security from the device. Cosens remarked that such virtualization could be a viable future strategy, but that designing future applications (and redesigning current ones) to this model would be an evolutionary process. Milford pointed out that some level of mobile device safeguards will be needed until we get to the point of completely virtualized applications. The council recognized the increased risk of mobile devices. McCourt favors no exception for only using Outlook web access because information seems to get on these devices in spite of intentions to the contrary. Advocated that safeguards such as this should be required for all mobile devices.

Domain 9 Overview - Information Systems Acquisition, Development, and Maintenance (20 minutes) – Tom Davis & Jim Thomas

See [https://protect.iu.edu/privacy/program/safeguards/9](https://protect.iu.edu/privacy/program/safeguards/9)

Davis introduced Jim Thomas Director of the Enterprise Business Systems within the Enterprise Software group in UITS.

Davis walked the council through an overview of this domain by section. This is a Domain that can be easily confused with Domain 7. Domain 7 is more about the safeguards protecting the networks, operational backups, and ensuring appropriate operating procedures. Domain 8 is more about managing the operating systems and application software whether it’s developed, purchased, or modified (during the whole life cycle). Reviewed objectives of this domain. Davis also detailed some of the tools we have available such as network vulnerability scanning, web application scanning, and Secunia personal software inspector (which helps keep workstation applications up-to-date).

Thomas talked about responsibilities of his group and how it handles the application development/acquisition process/community source life cycle. The Enterprise Software group is responsible for software that is considered “enterprise,” which is typically large-scale applications used across campuses, by many users, with far reaching types of services. ES is composed of 3 divisions: Enterprise Business Systems (administrative, i.e. HR, Payroll, Financial systems, Research Administration, Purchasing, E-Commerce, etc.), Enterprise Academic Systems (faculty/student facing systems such as Oncourse), and Enterprise Services Integration and Delivery (middleware pieces, core services, workflow, OneStart, etc.). Enterprise Business Systems doesn’t have a formal secure coding program in place, but does support opportunities for training in secure coding practices and has the expectation
that it’s part of the job of developers to know secure coding principles. There are also experienced expert developers that mentor other developers. Davis pointed out that one way hackers attack systems is to look for vulnerabilities in the software code itself. This goes directly back to the person/team that developed the code and highlights the importance of secure coding practices. We also have people developing systems (in the context of community source/development) who are not IU employees (who may not have training on secure coding, etc.). Davis also pointed out the need to protect production information during development and testing processes. Often, developers have access to a copy of production information in the dev/test environments which suggests similar safeguards should be in place to protect the dev/test environments (as those in place to protect production). Thomas acknowledged that there are some additional risks to think about w/contract developers/open source developers, but that open source also gets more eyes looking at the code, and other people can point out/identify problems, that is, collaborative development has the potential to improve security problem identification. Pointed out that the KUALI development infrastructure built to develop the code, helps reinforce good practices. Thomas explained the concept of development, testing/QA, and production environments and the iterative process of testing - culminating in an acceptance/sign off of an application before moving it into production. This is a formalized process within Enterprise Software. Developers themselves can’t make changes in production. That’s done by a different group – Production Services. So, there is some separation of duties. Rives asked whether maybe something should be added to an earlier domain (under affiliates in Domain 5), since these software development partners (i.e. Kuali project and other 3rd parties) are potentially accessing copies of production data in dev/test environments.

• Domain 10 Overview - Incident Management (20 minutes) – Kim Milford and Jonny Sweeny
  - See https://protect.iu.edu/privacy/program/safeguards/10
  - Milford walked the council through an overview of this domain by section, reviewed domain objectives. Sweeny described how this process currently works in the UIPO’s Incident Response function. This is a fairly sophisticated and well-tested process at a university level.
  - McCourt asked whether Incident Response helps people who have had their machine hacked learn how to prevent it from happening again or determine how it was hacked. Sweeny said because the numbers are so large we don’t have the resources to determine how every machine is compromised, only those involved in the worst incidents. However, the causes are generally the same (i.e. lack of patches, antivirus software, running as an admin account, visiting “questionable” web sites, installing Trojan software, etc.). So often, while we don’t get into the specifics of how a machine was compromised, we do give direction on how to rebuild the machine, use it responsibly, and promote the use of a number of tools to keep “bad things” from happening in the future.
  - Rives suggested that maybe, as part of user education, there could be a way to communicate actual incidents that have occurred to help make the potential consequences/benefits of security practices more real and relevant to users.
  - Lavagnino pointed out that one of our biggest challenges is our decentralized environment, and how do we cause the right things to occur within this decentralized context. We seem to be approaching a game-changing time when some things may just have to be required to access certain information. A base standard/suite of essential safeguards could be one approach.

• Wrap-up and Next Steps (10 minutes)
  - Next meeting: December 12, 2011
  - See action items below.

Action Items/Assignments
A1: Members asked to review (and have experts in their respective units review) domains 8 to 10 and provide feedback on languages, corrections, suggestions, additions, etc. for those domains and send to Lavagnino prior to 12/12/11 meeting if possible. Identify anything that should have group discussion.

A2: Members asked to prioritize gaps for Domains 8-10 with respective experts. Identify top 3 gaps in each domain. Will do gap prioritization small group exercise at next meeting.

* Note that all action items from previous meetings have been completed.

Parking lot

* Note that all parking lot items have been captured to the UISO Wiki or the IS&P Risk Council Oncourse Wiki. Going forward, the UISO Wiki will be used to maintain domain gap lists and the IS&P Risk Council Oncourse Wiki will be used to maintain potential agenda items.

Attachments/Reference

See Oncourse for meeting handouts.

See Information Security & Program at - [http://protect.iu.edu/privacy/program](http://protect.iu.edu/privacy/program)