Committee Name: Information Security and Privacy Risk Council

Date of Meeting, Time, Location: 10/26/2011, 3-5 PM (ended 4:35), Poplars 017, Video Bridge 223739

Attendees in person: Tom Davis (Chair), Merri Beth Lavagnino (Co-Chair), Eric Cosens, Dan Rives, Doug Wasitis, Jeff Lambright, Mary Frances McCourt, Sherrie Denney

Attendees via video: Marsha Gonzales, Joe Scodro, Philip Cochran, Kim Milford

Attendees via audio: none

Absent: Jim Kennedy, Jill Schunk, Mike Gardner, Joan Hagen, Chris Viers, Scott Wilson

---

Agenda/Discussion

Call to Order and Approval of Minutes (5 minutes)

- T. Davis called the meeting to order. Meeting feedback form was distributed. Minutes from previous meeting were approved.

Old Business and New Business (10 minutes)

- T. Davis – Domains 1 & 2 were reviewed at the last meeting and we’ve gone through and accumulated all the gaps identified in the gap documents. Our intent is to review all the domains, identify gaps, and prioritize gaps – to guide project work in our office and the work of the council going forward.
- Kim Milford – update from recent Committee of Data Stewards (CDS) meeting (10/24).
  1. CDS reviewed the 3rd party assessment proposal and is working on the associated policy. For critical information the plan is to require a security assessment of the 3rd party and data steward approval. For limited access/restricted information, the plan is to require standard contractual language.
  2. The Business Intelligence Governance group is looking for more clarification of “gray” areas. The term “public” was discussed as it is used to describe our least risky data classification. It’s a term that carries intrinsic meaning and causes some confusion. ‘Public’ does not mean information classified as such can simply be shared with anyone. CDS is considering redefining the term and evaluating appropriateness of other terms/names for that classification. “Disclosable” (or “potentially disclosable” – because “disclosable” is used in some law as a term of art, like “public” is in FERPA) is an alternative term that has been suggested. Information classifications were reviewed with the council (from - http://datamgmt.iu.edu/classifications.shtml). Tom Davis mentioned idea/advantage/value of extending information classification model to all types of university information, not just institutional information.
  3. CDS will soon be engaged in new education/awareness efforts.
  4. Will be classifying more data types, inventorying where data is stored.
  5. Passport and VISA numbers were classified as “critical.”
• Jenny Kincaid is expected to attend the December meeting and talk about the Policy Advisory Council.

Domains 3 and 4 - Review and Prioritization of Gaps (30 minutes)

• General comments/discussion of domains 3 and 4: Mary Frances commented that asset management domain seems very focused on information and physical assets. Doug Wasitis – domain 3 gaps list question related to 3rd bullet (i.e. indentifying all external 3rd party relationships, etc.) - is that even doable? Merri Beth Lavagnino – suggested that maybe we identify the most risky 3rd parties and manage those. Scodro – agreed w/ Wasitis’ comment and that such an inventory should be risk based. Gonzales commented that it would be difficult to get an inventory of business associate agreements because they come in through different avenues/channels. Furthermore, BA language can be embedded in a grant or contract instead of being stand alone. Main areas that would have such information would be grants/contracts, legal, purchasing, and research compliance. Scodro – d3 – ISPP25.1 – thought it was a good document, but it’s a very lengthy document. It’s a worthwhile document, but very dense. Lavagnino – someone suggested a page for each role in that document. That’s another suggestion of how to organize it. Mary Francis – found something similar with PCI-DSS. People just wanted to be told what to do, “where’s my checklist.” Gonzales – d3 – gaps (last bullet under internal organization gaps) – on the part where we have “new employees sign agreements” for sensitive data – wouldn’t it be wise to remind everyone that they may come into contact with such information and not just certain populations? Lavagnino – we have university-wide use agreement for access to information and information technology. As of 2009 the CDS asked that every employee sign the agreement, not just people with access to institutional systems. The reference here in the program is intended to be separate - such as when units have people sign special agreements that relate to their specific sectors (that was the intent of that gap – need to clarify language to indicate that it’s an additional layer). Rives – another possibility and something done in HR – many units handle confidential data that’s NOT electronic. So, HR has an additional confidentiality agreement that is much broader than what is in a system. Also, we have a large number of people associated with the university that are NOT employees. How do we deal with these people? Domain 3 – one thing he added as a gap – is regular intervals of education, maybe with some testing.

• Domain Gap prioritization exercise – council members paired up for 5-10 min. to discuss the domain gaps they came up with and to identify the top 3 gaps. 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 5 Overview - Human Resources (30 minutes) – Davis

• People are so important they have their own domain in the program.
• Standards divide safeguards into 3 time periods: prior to employment, during employment, change employment (including termination). Come from ISO standard.
• Rives pointed out that background checks only apply to some employees. With all the affiliates we have (a large number/many people), what we have in this domain only just begins to cover things. Safeguards are most often up to hiring managers to match people with positions (adequately screen candidates). Background checks are only done to verify after an offer has been made. Is there any guidance for unit managers as to how to screen employees? Who owns affiliates? How do we deal with/apply these safeguards/goals to non-employees?
• Cosens – pointed out that this domain is organized by life cycle – regardless of how people are associated with the university. So, as we go through the domain keep the life cycle idea in mind and how that might also apply to affiliates, contractors, etc.
Davis – ISO details 3 goals prior to employment:
  o security roles/responsibilities of people should be defined/documentd relative to security policy,
  o screening/background verification checks should be carried out (proportionally w/risk),
  o people should agree to terms of employment that include information security dimensions.

Scodro – the university sort of transfers the last goal to the user agreement.
Rives – the job application is a principal source of information for hiring managers to make decisions. Those managers make decisions based on that information and may make poor decisions based on that information.
Davis – perhaps more resources for hiring managers would be helpful.
Scodro – Could address by making a category of employment and under that subcategories of hiring/ongoing/termination to cover the life cycle. Then have an affiliate category and a vendor category (with similar life cycle subcategories). Big gap with affiliates – how do we define, measure, and regulate?
Lavagnino – we will reorganize and flesh out the affiliate and vendor categories – probably identifying more gaps in the process. Need to think about this domain further. Will work on domain with three types of people (with people from HR for staff and hourly).
Cosens – highlighted need to think about affiliates in a couple of different ways – those sponsored by university employees and those who are part of affiliated organizations.

Domain 6 Overview - Physical and Environmental (15 minutes)

• Broken into two sections
  o Secure Areas – addresses how we protect buildings/rooms/spaces at university. Examples: video surveillance, card access control, etc.
  o Equipment Security – addresses how we are protecting university equipment through its life cycle.
• Reviewed domain objectives
• Scodro – doesn’t see anything about plans/drawings of bldgs. Who protects those and how? Davis – held and managed by VP Morrison’s group. Do we have the appropriate safeguards around these digital AND paper. Milford – could consider cross referencing to business continuity from this domain.
• Reviewed currently identified gaps list. Has been some work on video surveillance policy and facility design standards relative to security/safety (base bid standards).
• Rives – thinks this domain is important since the university has so many buildings and since we are so decentralized (i.e. information is stored in many locations).

Domain 7 Overview - Communications & Operations Management (20 minutes)

• This domain addresses correct and secure operational management of systems to protect information.
• Sections are: Operational Procedures & Responsibilities, 3rd Party Service Delivery Management, System Planning & Acceptance, Protection Against Malicious Software, Back-up, Network Security Management, Media Handling, Exchange of Information, E-commerce Services, and Monitoring.
• Reviewed domain objectives.
• We have the most safeguards currently deployed in this domain because we have the most experience doing it.
• Reviewed currently identified gaps list.

Wrap-up and Next Steps (10 minutes) – copy from last and see recording.
• Please return feedback meeting forms.
• Next meeting on 11/29/11.

**Action Items/Assignments**

A1: COMPLETED. Philip Cochran and Joe Scodro volunteered to identify a central, face-to-face meeting location for IUPUI attendees. Determined that Phil was going to continue to join from his office and the admin assistants for Joe and Marcia are handling obtaining a room for them.

A2: COMPLETED. Delegates were requested to complete the meeting feedback survey and send to Merri Beth.

A3: COMPLETED. Review Domain 1 – provide feedback and identify gaps – (all).

A4: COMPLETED Review Domain 2 – provide feedback and identify gaps – (all).

A5: COMPLETED. Look at the different formats of Domain 1 and Domain 2 (paragraph vs. table). Which format do you prefer? (all)

A6: COMPLETED. Send a pre-meeting reminder about 24 hours before each meeting to the council members to review meeting handouts and minutes. (co-chairs)

A7: Lavagnino will work on revising the “cost/benefit” language in Domain 1.

A8: Lavagnino/Davis will compile/maintain domain gaps list/prioritization.

A9: Delegates were requested to complete the meeting feedback survey and send to Merri Beth.

A10: Delegates were requested to review Domains 5, 6, & 7 for feedback on the content at our next meeting, and to identify gaps.

A11: Delegates were asked to think about other groups with which it might make sense for this council to coordinate.

**Parking lot**

P1. Discuss how to best publicize this Council.

P2: Discuss how to improve communication about new policies, critical policies, etc., for example, could we use an Onestart popup?

P3: Discuss how we avoid losing valuable historical data which is only in employee’s personal email accounts.

P4: Discuss how risks that cross functional areas, depts., campuses, schools, etc. are being addressed.

P5: Suggested Risk Domain applications for the IS&P Risk Council:

   i. Identify “significant” risks.
   ii. Assess those risks (i.e. likelihood, impact, speed of onset, mitigations, preparedness, residual risk). Use an agreed upon process and tool.
   iii. Govern management of risks.
See Oncourse for meeting handouts.

See IS&P Program at - http://protect.iu.edu/privacy/program

For Gap lists By Domain, see Oncourse IS&P site in Resources – Gap Lists by Domain

For domain 5, 6, & 7 language see:
- https://protect.iu.edu/privacy/program/safeguards/5
- https://protect.iu.edu/privacy/program/safeguards/6
- https://protect.iu.edu/privacy/program/safeguards/7