

Committee of Data Stewards

7/23/08

**Discussion Items**

D1) Reports by subgroups

- a. Executive – much of what is discussed in this group is reports from these subgroups. Provide advice on goals, and talk generally about how the groups are working and if there are areas we need to concentrate on. Provide direction and advice.
- b. Policy – Kip Drew has sent her first draft of DMO3 to eliminate redundancy and get it in shape as the overall policy document (7/21/08). She will now take the other documents and turn them into more implementation or appendices documents. This subgroup will now schedule another meeting to discuss this policy and appendices. Phil asked if a retention policy should go to the Policy Subgroup or come from the Retention Subgroup; Steve indicated that the substance would come from Retention and then go to Policy for finalization process. Should Policy Group consider where we have gaps in policies and what we need? That is on the agenda for the Policy Group – Mark says look for places where we don't have guidance of some sort – keep policies fairly constant (don't change easily). Guidance documents might change more often.
- c. Awareness/Education – Don reported on two major bodies of work. 1) The next step in communicating with enterprise applications users, similar to the communication that went to IUIE users last fall by Mark's office. Request to get user agreement updated and indicate if this access is still needed. Mark identified two other groups – people that use enterprise systems or applications; the other audience is anyone who has access to institutional data – this is a very broad population and does not imply only electronic data. Committee provided Mark with input on how to communicate with these enterprise application users – hopefully customized to indicate which applications a user has access to. Try to ascertain whether or not users still need this access. Is this possible technically; left it to Mark's staff to determine if this is possible and how.
  - a. Merri Beth, Mark and Phyllis met today to seek user database lists from the enterprise applications with some criteria around them; i.e. we don't need all users of TIME, but only users who approve and have higher authority in TIME. Barry asked if this is not the list of people who use safeword card? Mark indicated that is not true for all systems. The CDS might need to revisit this decision which was made in the early days of the DS. Mark indicated that the CDS needs to have a discussion as to whether we need Safeword card at all! Is the risk worth the current cost?
  - b. We talked about whether or not we need more than one communication; we are going to try to have only one which is customized. Send them to a webpage where they can see what they have access to and possibly even their UA agreement date, and passphrase change date.

Committee has an interest in having ALL employees sign a UA – this is a general recommendation, but nothing of substance was decided. Might this be part of employee orientation? This might be better discussed by CDS as a whole. The second topic was where we need to go in general with Awareness and Education; Merri Beth provided a "roadmap" with stops along the way and a discussion of the differences between the various steps in Education/Awareness/Training, etc. Committee asked Merri Beth to try and map these across a continuum – the spreadsheet; major categories of the DS responsibilities at a high level. Decided we need a definitive list of "red hot" data elements. Once identified, fit into spreadsheet and decide what types of awareness/education was needed based on this information. SSN, Bank Numbers and PINS, IN driver's license, student loan info, passport info, passwords, etc.

Phil asked about where Records Management fits into this project. He teaches a course in HR every year which is a drop in the bucket for this type of education; trying to find ways to get people to have a better awareness of their responsibilities. Retention/Preservation group needs to make a recommendation so other groups can bring that to fruition. Expand the concept that Merri Beth and Beth Cate have used for general security awareness. Don pointed

out that we need a definitive list of data elements because adjectives alone become too vague or general; not all of the restricted data elements but possibly a subset.

- d. Retention/Preservation – struggling with scope of retention principles. Feeling of the groups is that the operational areas have a good idea of what they need to keep and for how long; they do not necessarily get rid of it after that time expires though. Asked each of the functional areas to indicate what types of documents they require to be kept. This led to a broader discussion to include databases, e-mail, etc. This changes the discussion somewhat. How do you determine which e-mails to archive and then, how do you archive them? Project collaboration systems might help with this; concept of an operational archive that would allow users to place documents, data into something other than Phil's traditional Archive. How would we deal with databases; rows, data elements, etc.? Mark indicated that we need to tell UITs that this is a priority, for instance if we need a way to archive e-mail, and ask them to take action to provide this ability and environment. There is an add-on to Exchange which facilitates this, but it is a very expensive option. If CDS could come up with functional requirements, this could be added to the next E-mail proposal (this will occur in the next 6 months). We have been looking at this rather holistically; is that appropriate? Don indicated that you might need to start with some sort of "imperative" so that we can take immediate action. Does this exist within this committee? Should be able to break off certain elements such as policies according to Phil.

Vince indicated that in talking with people, archiving of e-mail seems to be a major issue. If we could identify a needs assessment around e-mail archiving, might this give us a place to start? Interplay between asking people to do something without providing a way for them to do that is difficult. Mark indicated that we can make a presumption that IU is losing valuable information in e-mail communications. People still struggle with what to keep and how to do that? This group might come up with a couple of short-term things to do as a place to get started. Work concurrently on broader issues. CDS cares about institutional data contained within e-mail, not necessarily e-mail messages in general. Marilyn pointed out that Purchasing has been aware of this for a very long time; they have an archiving system of their e-mails which anyone within Purchasing can access instead of a person's individual e-mail archive. They scan documents as well. Phil indicated we need an enterprise solution. There is a stewardship council within UITs that might take action on such recommendations. Dennis mentioned that many of the technology solutions work very well in a highly structured environment which is not an educational environment. Vince indicated that this is more about education and training than going out and buying an expensive system. Marilyn pointed out that according to Merri Beth's definitions, we start with Awareness. Barry asked if Legal Council has any regulations surrounding e-mail; the answer is no. E-mail can be a record just as a piece of paper can be a record; therefore it is subject to open records laws. Use existing laws and rules that exist and apply them.

- e. Laurie reported that Dan and Student Enrollment Services have been working to remove excess data from databases, masking SSN, etc., as well as removing unnecessary users from the access databases.

D2. & D3. Merri Beth and Tom provided a report of data-related incidents.

D4. Kevin Keough – **Compliance with Payment Card Industry –Data Security Standards – referred to as PCI-DSS - dated July 2, 2008**

The University processed - \$126 million of payment cards payments during fiscal year 2007 – 184 merchants processed 626,000 payment card transactions –

Our objective was to determine if the adequacy of the processes and controls that ensure compliance with PCI-DSS-

Our assessment was critical – and we had agreement that there were areas of non-compliance that needed immediate attention.

**Our findings included:**

There is not an adequate process in place to monitor and enforce PCI-DSS compliance

The Verisign Internet Payment Authorization System – IPAS – is noncompliant – this application process \$9 million – 114,000 transactions -18% of our payment card activity

We reviewed 5 of the 16 merchants who had requested exception - exception to centralized processing is granted by the Office of the Treasurer - all 5 were found to be noncompliant – These merchants – other than Ticketmaster application that recently June of '08 - upgraded to a PCI-DSS compliant solution – represent \$10.8 million – 86,000 transactions or 14% of our payment card activity –

We did not find that the Office of the Treasurer adequately challenged merchants requesting to use third parties to process payment cards –

**Actions planned:**

The Office of the Treasurer has a goal to continue to work in collaboration with UITS – ITSO and the Dept accepting payment cards to reach compliance by 12/31/08

For those Departments using 3<sup>rd</sup> party processors – if they are not compliant by 12/31/08 – their authorization to accept payment cards will be suspended until that time they have reached verifiable compliance –

We also completed a Transitional Management Review of the VPIT – couple of IT Policy and data related issues that made it to the Management Letter – these are not a report items – these comments are

1 – Disposal of IT resource that contain data – we did not find documentation of verified data removal actions taken for certain IT assets that were disposed of that were known to have stored sensitive data – What we asked to be done – is that the Committee of Data Stewards be charged with developing a media sanitation standards and guidance for all IT assets disposed of. We currently have 2 Purchasing Policies that provide guidance.

2 – One of the frustrations we have as Internal Auditors - & I would think that those being audited would have the same concerns – What are the expectations of the functional unit technician – we currently use IT-12 – but questions have been brought up about how enforceable these duties and responsibilities are – and how best should we be reporting our IT findings.

What I would like to see the Data Stewards do—develop a process that identifies – lists – and keeps current – what the duties and the responsibilities of functional unit technician are – and that requires documentation to be kept – an audit trail – of how the technician performs these duties and responsibilities-

Related to this, Mark is pushing back to compare what we do with “best practices”. Sometimes what they find do not always fit with higher ed but may work with corporate or government environment. Merri Beth, Mark and Tom are working on their own guidance to be used at IU. This will be something Audit can use in reviewing processes and procedures. Should media sometimes be destroyed because the data is so sensitive? What do we do about expensive hardware which we could sell on the open market; can't use DOD processes which might require destruction of the hardware?

D5. Reversed 5 and 6 – IUIE audit follow up – there will be a follow up within the next several months. Mark will go through the audit response with UITS AVPs, to get feedback and advice. Much of the response had to do with reforming the CDS and the various subcommittees. Good progress has been made on this imperative. IUIE staff will work with DMs to work through user access lists and get people who are no longer here out, and those who don't need this access removed. Item about unmasked SSN in datagroups and tables; Becky Gribble is working with DMs to get this taken care of for data in IUIE.

D6. FERPA changes – Kip reported that there have been a few changes – at the professional conference they were made primarily to codify guidance that was already in the process of being implemented. Spent a lot of time dealing with Health and Safety exceptions (emergencies) in the wake of Northern Illinois and Va. Tech instances; designed to help universities feel more comfortable about dealing with students with difficulties (such as emotional problems). Interpretation from Leroy Rooker that Student ID is sensitive; IUPUI wanted to put this on the front of the Student ID cards. DOE interpreted that we could NOT! Susan Langsdale and Beth Cate were talking to DOE about that.

D7. Representation for Faculty Data – Mark reported on this. There really isn't faculty data representation on the CDS; there used to be. Vince talked about some of the issues between IUPUI and the School of Medicine. Mark felt that once we get to the point of having to have this discussion we could include resources from SOM. Dan Rives raised the question about John Applegate and his new role; includes academic policy – might he be able to complement or give ideas of how to achieve this goal? He will be working on academically oriented projects and programs. We should ask him about who the best person might be to represent faculty data concerns; resolve via e-mail asap.

**Action Items**

A1) Determine the list of "red hot" elements (who responsible?)

A2) Kip to give presentation on Open Records Law at next CDS

A3) Mark will contact John Applegate about the appropriate person to represent faculty data on the Committee of Data Stewards