Notes-ConferenceCall-March-21-2011

notes, social identity call, 3/21/2011, risk assessment

Issues

-- how to assess risk on an SP site, and determine whether a social identity can be used

-- how does one communicate that such an assessment is needed ? how do we represent the result of that assessment, both in text, and in a machine to machine fashion

-- how to explain this to business owners, so they can put it in terms of their service... they may not be familiar with this more formalized risk assessment process

Target audience -- IT staff, business owners, security group

NOTES:

-- risk is inherent every time access is provided -- login to wireless, send threats via email....

-- business owners aren't familiar with the more formalized risk assessment processes; the equate facebook security with the security provided by other applications using password based mechanisms; anyone used to the facebook model might see our approach as "too heavy"
    -- important to make sure that business owners understand risks, and they have reccomendations on steps they can take to mitigate such risk....
    .. eg understand LoA, or data breach, credential compromise; owner decides if data requires different authN requirements

    -- UW presentation at I2MM on UW process, working with data owners on access to group data (eg membership, or send email to it)
        Balancing Risk and Opportunity for an Institutional Groups Service

http://events.internet2.edu/2011/spring-mm/agenda.cfm?go=session&id=10001722&event=1035

-- security office at some campuses is focused on "what happens if there's an incident" -- will they have enough logging etc to investigate
    -- if we learn that a social identity has been compromised, could they take it out of service quickly, and how to re-enable
    -- focus on "if there has been a compromise, would we look like idiots"
    -- in deciding whether an application should use social identities, one question to ask is -- have you done the due diligence, as to how to handle a case like this properly, rather than acting rashly with no thought or plan

-- even with IT staff, few people understand that authentication assertions in different protocols are different -- ie have different LoAs associated with them.

-- one campus noted -- in discussions with auditors about this new model, been struck by the degree of "reasonableness" from their side

    -- they really want a very good trail left, so can reconstruct what happened
    -- when they talk to business owners, they get warm and fuzzy when they hear that auditors are comfortable

-- there are lots of sites on the open web where zero LoA accounts can POST comments; due to abusive conversation is there a changing perception in the wider world regarding allowing this sort of posting on various web sites?
    -- can we identify criteria for why POSTing should require a linkage of account to a body....
    -- hopefully, reader would assign different perception to something posted from univ acct vs facebook acct

-- campuses often have policies related to abusive speech; creative expression vs keeping to the discussion; not aware of anyone who's looked at the role of identity; lots of policies around "must have netid to play in game X"...

-- there may be situations where start with low LoA, but then do something and need a step up
    -- example -- pre-admission person getting real enterprise issued identity
    more like account linking

    -- example -- SP running content mgmt site, ok for zero LoA users to view content; but, POSTing requires a higher LoA; what if site owner has to trace back after a POST of objectionable content

PROPOSAL -- social identities are only relevant when that sort of audit trail wasn't required; if it mattered, then social is inappropriate

-- assess risk by looking at the type of data in the system -- eg financial, personal data, legal (FERPA,)

-- UW, with a new student system, looked at risks around who can post grade data to the new site

-- would a campus allow a student to log in to do course work with a social identity...

-- chicago -- LMS, used by doctors not associated with Chi hospitals, hosp asserts that janeDoe@gmail belongs to this doctor...

- students working with state agencies, mentors at those agencies submit progress reports on student; some level of offialness with app; not a level 2; roughly comparable to submitting grades, tho; only have email addresses for the mentors; discussed giving UW identities to mentors...

-- staff member with a high LOA acct, taking a course, want to limit environments where high LOA can be activated....
-- associating a person with multiple accounts, with different LOAs

-- are criteria other than data type part of the equation ?
-- transactional context...
-- access policy is about r/o, open access, doesn't address whats kinds of protections are needed on updates

-- thoughts on how to categorize the various types of "accounts"
-- level zero -- IP addr
social -- at level one (russ would prefer trusting a paypal, rather than a facebook)
-- how to quantify that paypal is better than facebook ?
-- paypal, google both at LoA 1, because both use openid
campus identities mostly at level 2
RL -- some of those providers interested in LoA 3.....; would need fed gov apps at that level to interest them, tho...

--does anyone have a service where social identities can be used to login ?
UW -- lots of dept sites, described by UW person
pretty easy these days for someone to put up an app leveraging google
central IT doesn't necessarily hear about them
supplementing the traditioanl "create another ID on this site"
anyone using ProtectNetwork is engaged in this

PSU -- authN required in order to add a comment to a post ont he centralblog service

-- are there campuses with data driven policy ? data with certain characterisitcs needs certain LOA?

-- berkeley has such a policy -- certain types of data (eg SSN) requires a 2nd factor

-- cmu has some data policies, nothing addresses social identity

-- chicago -- nothing addresses social, but does require fac or staff affiliation

-- berkeley -- policy driven by specific data items; wants to see development of "categories of data "

-- osu -- have different classifications, policy written in terms of classes
data owner responsible for classifying data into a class; triggers protection characteristics (can it be public, how its protected on servers)

-- consensus -- expect new policies will follow std practice; expect it to be abstracted, tho and not get to "require a netid" level of detail

-- consensus -- technology change, terminology change occuring faster than policies evolve

ACTION ITEMS

-- figure out how to frame this discussion to bus offices