CaseStudyDiscussionNotes SaSp2012

**CaseStudy 1, Jaferian et al, 2009**

 Kelsey Bartiss, bkelsey <bkelsey@live.unc.edu>

impact of size of organization, amount of information. Biggest challenge of company?

At what point should formal IdM system be acquired? before or after (or as) it becomes a work overload?

Allen Bell, Bell, Allen Allen [bellma@live.unc.edu](mailto:bellma@live.unc.edu)

how to encourage people to follow protocols, e.g., record-keeping with requesting and granting access?

Given the mess they were in, were there smaller improvements they could have made, rather than the total overall? Is this a situation where agile methods would be appropriate?

challenge of collaboration with business folks, and convincing them that it was a crucial problem.

Melissa Harden,

existing complexity in accounts/access at the beginning. common to organizations?

value of easy success with task that everyone can see, in this case the password self-service.

What would this project look like at a smaller, less complex company?

What will the system look like later, in terms of maintenance, cost, efficiency, effectiveness, etc.

<also, how will they monitor to catch problems?>

importance of consistent and clear communication among departments; making sure those responsible for something understoon their responsibilities.

Katy Sandlin, Sandlin, Katy [ksand17@live.unc.edu](mailto:ksand17@live.unc.edu)

good thought to include link on open coding, sinc this is how they identified who needs what.

compare/contrast "digital identity" and "IdM". Apart from access, what does digital identity bring in modern organizations?

issues of "data guardianship" advantages, disadvantages?

early adoption. How could libraries/archives fit into assisting organizations with access issues?

How do same issues play out in other types of organizations?

workflow changes.

Megan Slemons,

liked the scoring system for selecting a vendor; criteria and degree of fit.

password self-service: immediate results, visible, investment in success.

Will Security Admin and IT employees' jobs change as a result? how?

Estimation problems: time, money, especially caused by not grasping the complexity of the system.

Challenges of getting people from different departments to work together.

MelissaTroyer,

possible utility of data guardianship in other organizations, e.g., library.

even with policy, is periodic review of individual accounts/access a good idea (an audit)?

how could they have gotten a better time estimate?

Is email the most effective way to communication with branches, employees?

risks, factors over which they had no control, e.g., the acquisitions, competition that vendor experienced.

Bin Zhang binzh [binzh@live.unc.edu](mailto:binzh@live.unc.edu)

standards and consistency during operations.

risks: if even a small role or permission guidelines are unclear, it can lead to problems.

Definition/functions of participant roles.

Other pre-requisites for deploying IdM solution?

**Summary to Discussion Leaders**

A summary of some of the points you raised about the case study is below. Remember that these are just to give you a starting point. You and your group should talk about whatever issues or questions grabbed your interest.

Impact of the organization:

Would the identity/access problem be different in a smaller organization? Would the analysis and implementation differ? Would the roles and their definitions/responsibilities differ?

What lessons are there for other types of organizations, e.g., libraries, universities, government agencies?

Communication Issues:

clear understanding of responsibilities, getting buy-in and cooperation from all departments, establishing a good relationship with the vendor.

Project Management:

Was the process inherently so complex, or did they make it more complicated than necessary?

Could they have solved the identity/access problems with smaller changes?

They underestimated the time it would take to design and implement the new system. Are there ways this could have been avoided?

Benefits of deploying an easy, visible, and successful part of the project (password self-service) as way of getting buy-in.

The Future:

Will IT and Security employees' jobs change?

Are there actions or policies that should be implemented to monitor the new system?