Cloud and IDM
Security & Policy Implecations

Cloud Security
Paul Schopis CTO
OARnet
InCamp
June 23, 2011
Columbus, Ohio

What is Cloud Computing?

Cloud computing is a style of computing using scalability, elasticity and Internet technologies. – *Gartner*

What is Cloud Computing?

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential **characteristics,** three **service models**, and four **deployment models**. - *The NIST Definition of Cloud Computing*

Ohio | OARnet

Concerns depend on who you are

- Consumers of a service
  - What is my provider doing to ensure my data is not compromised by someone else?
  - For users of public cloud services what can/must I do to ensure security and data integrity?
- Providers of a service
  - What assurances and services can I provide?
  - How do I know who you are?

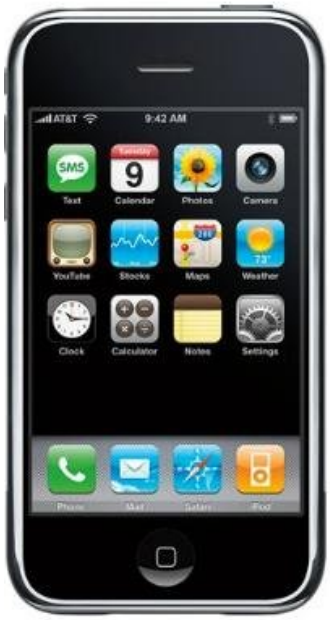
Ohio | OARnet

Concerns depend on who you are

- For both consumers and providers
  - What is it I'm trying to protect?
  - Does the level of data importance justify the expense?
  - In other words, does my institution/organizations have metrics, methods and policies to map data types on regular basis and assign risk and mitigation strategies etc?
  - Can IDM help me address these concerns?

Question

- Based on the offered definitions what is the most popular cloud solution/device ?



What's this mean?

- Nothing new really
- Historically technology has moved at a faster pace than security concerns
- BTW the iPhone/iPad iOS does
  - Have key based encryption
  - Ties key generation to the hardware making it uniquely identifiable (banks like that idea)
  - However only Apple's email takes advantage of it and since it decrypts on access anyone with a USB cable can defeat it

What's this mean?

- We now live in a world where consumer devices are used increasingly to access institutional data
- Most institutions do not have policies surrounding use of privately owned smart phones having sensitive data on them
- The old model of tight security around the perimeter is dying
- The notion of only "certified and supported" devices is dead

What's this mean?

- We need to get smart about how to control data
- We need to get smart about how to assign risk
- We need to get smart about how to create decision rights and accountability
- The good news is the "standard" IT governance models address most of these issues
- The bad news is ~80% of organizations have no governance or immature governance

Identity Management

- Make ID management an integral part of data governance
- Become familiar with the standards such as NIST SP 800-63 and OMB M-04-04
- In that context rationalize Level of Assurance (LOA) with access privilege and credentials
- Establishing LOA criteria is a major feature of Identity Federations.

OMB M-04-04

- Defines 4 levels of LOA
  - little or no assurance
  - Some confidence
  - High confidence
  - Very high confidence

NIST SP 800-63

- Maps 4 levels of LOA to required proof
  1. little or no assurance – None i.e. Facebook
  2. Some confidence – Document Presentation
  3. High confidence – Document verification
  4. Very high confidence – Appear in person, two govt' IDs, verified and capture biometric reference

Ohio | OARnet

Putting it together

Risk				
Reputation	Low	Mod	Mod	Hi
Financial	Low	Mod	Mod	Hi
Mission		Low	Mod	Hi
Info Disclosure			Mod	Hi
Safety		Low	Low	Mod/Hi
Legal		Low	Mod	Hi
Required LOA	1	2	3	4

Ohio | OARnet