Ohio | OARnet

Cloud Security

Myths, Legends and Reality

Cloud Security
Paul Schopis CTO
OARnet
Joint Techs

What this presentation is and is not

- It is an over view of ideas and strategies regarding cloud based systems
- The goal is to stimulate conversation and get us thinking about the emerging realities of the current environment
- It is not particularly technical because the issues are social, behavioral and governance
- I encourage audience participation

What is a cloud?

- **Cloud computing** is Internet based computing, whereby shared resources, software, and information are provided to computers and other devices on demand, like the electricity grid. – *Wikipedia*
- **Cloud computing** is a style of computing using scalability, elasticity and Internet technologies. – *Gartner*

Concerns depend on who you are

- Consumers of a service
  - What is my provider doing to ensure my data is not compromised
  - 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?
  - What assurances and services should I provide and what are the liabilities associated with both?
  - How do I know who you are?

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? (more on this shortly)

Question

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


AT&T
9:42 AM
SMS
Text
Calendar
Photos
Camera
YouTube
Stocks
Maps
Weather
Clock
Calculator
Notes
Settings
Phone
Mail
Safari
iPod

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

Oh No! He's become one of the suits……

- First steps are
  - Make a conscious decision to take a data inventory
  - Use that information to assign risk, the idea being match the effort to secure data against its value
  - Keep it simple there are only 3 kinds in most security models
    - Public – No restrictions
    - Limited – Not legally protected but may be proprietary and requires documented process to obtain
    - Restricted – Legally protected such as PII or critical operational information that could compromise security of made public
- Make sure there is a data lifecycle plan

Oh No! He's become one of the suits……

- Assign roles and responsibilities
  - Data Stewart – ultimately responsible for creating local policy or carrying out organizational policy. Final authority on access on data in their charge
  - Data Custodian – Systems or administrative personnel charged with enforcing standards on a daily basis
  - Data User – Users of data that are charged with applicable non-disclosure and adhering to acceptable use

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

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

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

Certifying Body for IDP

- ICAN
  - Identity Credential and Access Management Subcommittee
- Three entities
  - Kantara
  - Open ID Exchange
  - InCommon

If you are a consumer

- What assurances does your provider accept?
- What certifications does he process?
- What contractual obligations for management and security does vendor offer?
- What are disentanglement provisions for non-performance?
- Will they allow you test?
- Who owns the data?

If you are a consumer - OARnet example

- What certs does your provider accept?
  - OARnet must provide LDAP or AD
- What certifications does he process?
  - HIPPA compliant
- What contractual obligations for management and security does vendor offer?
  - Full
- What are disentanglement provisions for non-performance?
  - Termination without penalty
- Will they allow you test?
  - yes
- Who owns the data?
  - OARnet

If you are provider

- What level of services do you offer?
- Client manages which services?
- What liabilities are you willing to accept?
- Do you have well documented procedures and processes appropriate for the service level?

If you are provider OARnet example

- What level of services do you offer?
  - Gold (fully managed), Silver (Amazon like) and Bronze (Resource pools)
- Client manage which services?
  - Depends on which service
- What liabilities are you willing to accept?
  - Insist that client follow all state & university policies
- Do you have well documented procedures and processes appropriate for the service level?
  - Gold (yes), Silver (working on it), Bronze (NA)

Questions?

Paul Schopis

pschopis@oar.net