How Credit Unions Are Taking Advantage of the Cloud

CUNA Technology Council Conference
September 2013

Randy Romes, CISSP, CRISC, MCP, PCI-QSA
Principal, Information Security and Financial Institutions
CliftonLarsonAllen
Our perspective...

*CliftonLarsonAllen*

- Started in 1953 with a goal of total client service
- Today, industry specialized CPA and Advisory firm ranked in the top 10 in the U.S.
- Largest Credit Union Service Practice*

*Callahan and Associates 2012 Guide to Credit Union CPA Auditors.

CliftonLarsonAllen’s credit union practice has recently grown to over 100 professionals including more than 20 principals. The group focuses on audit, assurance, consulting and advisory, information technology, and human resource management for credit unions across the country.

www.larsonallen.com – news release
Overview

• What is “the cloud” – Terms and Definitions
  – Standards, Service and Deployment Models
• Benefits
• Risks
• Things to think about...
• Resources and References
Definition of a Secure System

“A secure system is one we can depend on to behave as we expect.”

Source: “Web Security and Commerce” by Simson Garfinkel with Gene Spafford

- Confidentiality
- Integrity
- Availability
What is the Cloud?

• Is it a clever marketing term?

• Where is the cloud?
The Original “Cloud” Computing Model?

- Mainframes
Cloud Version 2.0?

- Thin Clients (Citrix, RDP, etc...)
Today's Forecast: Cloudy or Clear?

- Hosted service or process all the way to hosted infrastructure.
Cloud Standards

• National Institute of Standards and Technology (NIST) definition of cloud computing published October 7, 2009:

“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.”
Three Cloud Computing Service Models

• Software as a Service (SaaS)
  – Capability to use the provider’s applications that run on the cloud infrastructure.

• Platform as a Service (PaaS)
  – Capability to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider.

• Infrastructure as a Service (IaaS)
  – Capability to provision processing, storage, networks and other fundamental computing resources that offer the customer the ability to deploy and run arbitrary software, which can include operating systems and applications.
Cloud Computing is about “Multi-Tenancy”

- Multi-Tenancy implies the use of the same resources or application by multiple businesses/user communities/consumers that may belong to the same organization or different organizations.
Cloud Computing Service Models

• The **KEY** takeaway for cloud architecture is that:
  - The lower down the stack the cloud service provider stops --
  - The more capabilities and management the users are responsible for implementing and managing themselves
What does that mean?

• Cloud computing means an increased need for:
  ➢ Good polices
  ➢ Clear communication between the provider and the consumer of the services
  ➢ Ownership and governance of the relationship with the provider
Cloud Computing Deployment Models

- **Private cloud:**
  - Operated solely for an organization
  - May be managed by the organization or a third party
  - May exist on or off premise

- **Community cloud:**
  - Shared by several organizations
  - Supports a specific community that has a shared mission or interest
  - May be managed by the organizations or a third party
  - May reside on or off premise
Cloud Computing Deployment Models cont.

- **Public cloud:**
  - Made available to the general public or a large industry group
  - Owned by an organization that sells cloud services

- **Hybrid cloud:**
  - Composed of two or more clouds (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)
Benefits

• Cost
• Administration
• DR/BCP
• Compliance
Risks

• Vendor Risks
• Governance Risks
• Data Risks

• Who has your data?
• Where is your data?
• Who has access to your data?
What Credit Unions Are Doing Mobile Banking

• Example

This is essentially a web server for the mobile devices to connect to.

Also need controls on the dedicated link...

• Pros
• Cons
• Lessons Learned?
What Credit Unions Are Doing
Enterprise Applications
Key/Core Vendor Supplied...

• Vendor supplied application system within organization for check imaging and processing
  – VPN connection between FI and vendor
  – Data (images) sent to datacenter
  – Processing done at vendors data center

• 3 Primary categories of issues
  – Architecture
  – Authentication
  – Weak/default vendor configurations
What Credit Unions Are Doing

Enterprise Applications

Key/Core Vendor Supplied...

- Architecture - Wide open site-to-site VPN connection to the vendors datacenter
  - No restrictions or filtering of traffic
  - Default passwords and anonymous FTP
  - Missing Microsoft updates (some more than 4 years old)
  - “Visibility” through data center to other FIs
What Credit Unions Are Doing
Enterprise Applications
Online Accounting/Management System

- Example of attack into financial management software
- “In the cloud” application for staff
- Defaults?
- Logging?

- Lessons Learned...
What Credit Unions Are Doing Online (Secure) Backups

• Backup Appliance
  – Highly efficient/automated
  – Local copies and in-the cloud
  – Ability to restore w/in cloud (DRP/BCP bonus)

• Vendor managed
  – Remote access...
What Credit Unions Are Doing Online (Secure) Backups

- Recent conference
  - Company X offers online, secure back up to the cloud
  - Company X has grown “over 300%” in the last year
  - Best of all, Company X now provides online, secure, cloud based back up for Company Y – one of the larger Core hosting company providers

- Where does the outsourcing chain end?
- How many FI’s using Company Y know where their data is
What Credit Unions Are Doing
Enterprise Communication - Email

• Recent client experience
  ➢ 18 months ago we outsourced our email to a cloud based email solution with Company A
  ➢ 6 months ago Company A was purchased by Company B
  ➢ 2 months ago Company B was purchased by Company C

❖ I don’t know where my data is...
❖ I don’t know who has access to my data...
❖ I don’t know where my data is backed up at any more...
❖ I don’t know...
What Credit Unions Are Doing
Bring Your Own Device (BYOD)

• Data classification
• Standards
  – Hardware and Software
  – Process and Storage
  – Acceptable Use
• Controls to support the above
  – Preventative controls
  – Administrative controls
  – Monitoring controls
Examples in the news...

“Cloud Computing Service Outages in 2011”

- Playstation Network 4/21/11 25 days
- Amazon Web Services 4/21/11 4 days
- Twitter 2/25, 3/16, 3/25, 3/27 periodically
- Gmail and Google Apps 2/27/11 2 days
- Intuit Service & Quickbooks 3/28/11 2-5 days
Examples in the news...

- Google: “cloud service outage”
- **Microsoft Windows Azure Cloud Suffers Outage; Blame Leap Year**
- Feb 29, 2012 – Microsoft Windows Azure, the software company's cloud computing service, has been suffering through a lengthy outage today, preventing ...

- **Amazon gets 'black eye' from cloud outage** – Computerworld
- Apr 21, 2011
  Keith Shaw chats with Network World's Jon Brodkin about the Amazon EC2 cloud service outage that ...
Cloud Computing Controls

• The overall control domain is the same as an in-house IT environment, the challenge is to figure out who is doing what.

• Controls in the cloud computing environment may be provided by the consumer/company, the cloud service provider, or a separate 3rd party.

• SSAE 16 SOC2 or SOC3 report from service providers
  – Stick with someone familiar with FI’s…
Evaluate the Control Environment

Security Control Model

Applications
- SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.

Information
- DLP, CMF, Database Activity Monitoring, Encryption

Management
- GRC, IAM, WA/VM, Patch Management, Configuration Management, Monitoring

Network
- NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth

Trusted Computing
- Hardware & Software RoT & API's

Compute & Storage
- Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking

Physical
- Physical Plant Security, CCTV, Guards

Compliance Model

PCI
- Firewalls
- Code Review
- WAF
- Encryption
- Unique User IDs
- Anti-Virus
- Monitoring/IDS/IPS
- Patch/Vulnerability Management
- Physical Access Control
- Two-Factor Authentication...

HIPAA

GLBA

SOX
Risk Assessment: What to Consider

• **Due Diligence**
  – Review service providers SSAE16 SOC report which provided a third party opinion on the suitability of the design and operating effectiveness of the controls.

• **Vendor Management**
  – CU has clear contractual relationship with the service provider which defines the responsibilities for both the vendor and CU.
  – Internal management of the service provider is assigned and managed within the IT area to monitor services and compliance.
Risk Assessment: What to Consider

- **Audit**
  - CU has defined internal controls for the IT area and has actively reviewed the impact of cloud computing against the defined controls, updating or creating new controls as needed.

- **Information Security**
  - The cloud services SSAE16 SOC report defines the information security practices provided to CU.
  - CU has documented the internal processes what data can be held in cloud environments, handling, backup, monitoring, and other data centric controls for this environment.
Risk Assessment: What to Consider

• **Legal, Regulatory, and Reputation Considerations**
  – CU has clearly defined what information and services are provided within the cloud services environment.
  – Contracts are in place which define the service providers obligations.

• **Business Continuity Planning**
  – Reviewed the service providers SSAE16 SOC report which describes the cloud service providers BCP/DRP planning and operational backup, and incident response control environment.
Things to do...

- Risk Assessment (process – NOT point in time...)
- Cost benefit analysis
- Vendor due diligence
- Scrutinize contracts
- Ongoing vendor management
- Be rigorous about where your data is
- Understand vendors responsibility and YOURS
- Remember basic security tenants
Definition of a Secure System

“A secure system is one we can depend on to behave as we expect.”

Source: “Web Security and Commerce” by Simson Garfinkel with Gene Spafford

• Confidentiality
• Integrity
• Availability
Questions?
Thank you!

Randy Romes, CISSP, CRISC, MCP, PCI-QSA
Principal
Information Security Services & Financial Institutions
Randy.romes@cliftonlarsonallen.com
888.529.2648
References & Resources

- Google: “Managing the risks as you outsource to the Cloud”
- [www.ISACA.org](http://www.ISACA.org)
  - Good source of audit and assurance templates
Cloud Audit and Compliance References

- NIST csrc.nist.gov/publications/pubsSPs.html
  - NIST Special Publication 800-144 Guidelines on Security and Privacy in Public Cloud Computing
  - NIST Special Publication 800-145 The NIST Definition of Cloud Computing
  - NIST Special Publication 800-146 Cloud Computing Synopsis and Recommendations
  - NIST Special Publications 800-53 Recommended Security Controls for Federal Information Systems and Organizations
Cloud Audit and Compliance References

• Cloud Computing Security Alliance
  cloudsecurityalliance.org
  – Security Guidance
  – Cloud Controls Matrix
  – Top Threats to Cloud Computing Report

• ISACA www.isaca.org
  – Cloud Computing Management Audit/Assurance Program
Risk Assessment Outline: A Quick Approach

How does Confidentiality, Integrity, Availability change if all or part of an asset is handled in the cloud.

• Identify the Asset in the cloud
  – Data
  – Applications/Functions/Processes

• Evaluate the Asset: How would the business be harmed or impacted if
  ◊ The data became widely public and distributed
  ◊ The provider accessed the data
  ◊ The data or function was manipulated by an outsider
  ◊ The function failed to provide expected results
  ◊ The data was unexpectedly changed
  ◊ The data or function were unavailable
Risk Assessment Outline: A Quick Approach

• Determine the Cloud Deployment Model
  – Public
  – Private, Internal / External
  – Community
  – Hybrid
Risk Assessment Outline: A Quick Approach

• Map out the Data Flow
  – Public
  – Private, Internal
  – Private, External
  – Community
  – Hybrid
Risk Assessment Outline: A Quick Approach

• Legal issues
  – Where is the data?
    ◊ Is it here?
    ◊ Another State?
    ◊ Another Country?
  – eDiscovery:
    ◊ How do you identify all documents that pertain to a case?
    ◊ Possession, Custody and Control: How do you control and make available data that is not in your own systems yet is your data?