LBMC INFORMATION SECURITY

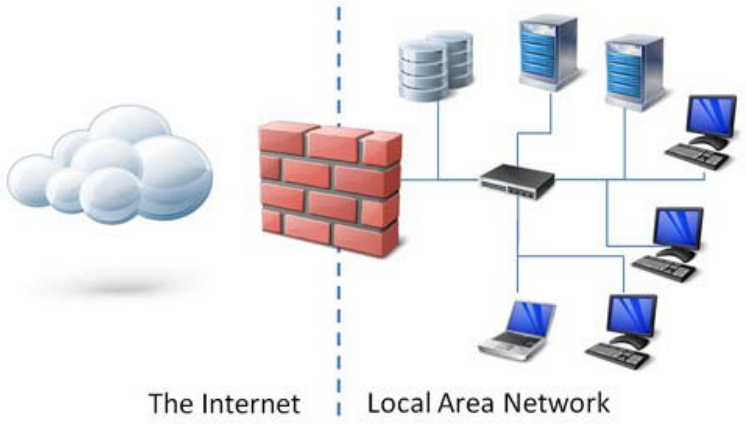
Cloud Security – Are the Risk Real?

Chattanooga Tax Practitioners | **January 13, 2016**

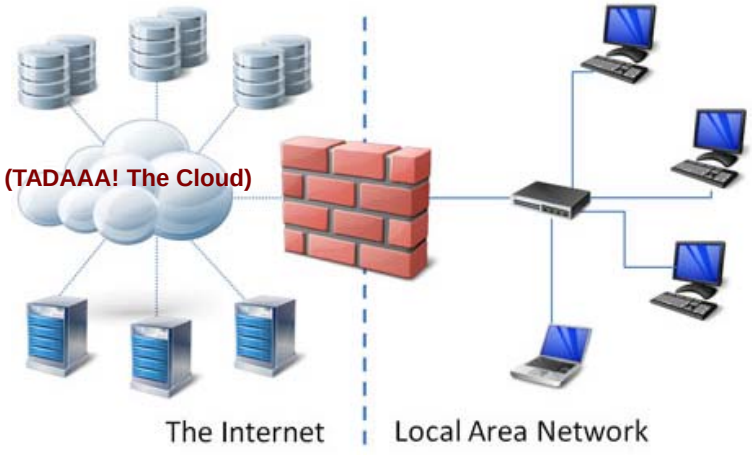
What is Cloud?

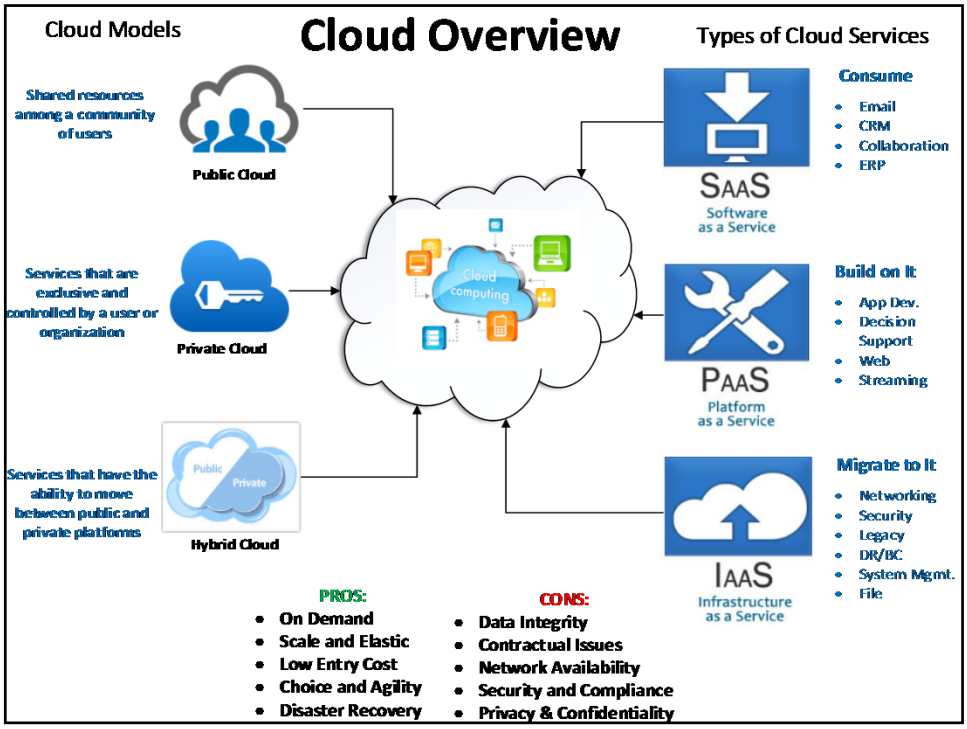
A style of computing where scalable and flexible IT services are delivered to external customers using Internet technologies in a way that allows them to be cost effective and responsive to customer needs while taking advantage of economies of scale.

Traditional Computing



Cloud Computing




Cloud Models
Cloud Overview
Types of Cloud Services
Shared resources among a community of users
Public Cloud
Services that are exclusive and controlled by a user or organization
Private Cloud
Services that have the ability to move between public and private platforms
Public
Private
Hybrid Cloud
Cloud computing
SAAS
Software as a Service
Consume
Email
CRM
Collaboration
ERP
PAAS
Platform as a Service
Build on It
App Dev.
Decision Support
Web
Streaming
IAAS
Infrastructure as a Service
Migrate to It
Networking
Security
Legacy
DR/BC
System Mgmt.
File
PROS:
On Demand
Scale and Elastic
Low Entry Cost
Choice and Agility
Disaster Recovery
CONS:
Data Integrity
Contractual Issues
Network Availability
Security and Compliance
Privacy & Confidentiality


Cloud Has a Dark Side too…

Are the Risk Real?

Cloud Security Statistics

> 75% of IT decision makers are "extremely anxious" about security using cloud-based services -- yet 79 percent of U.S. enterprise execs (70 percent globally) are adopting cloud."

- Cloud Security Alliance 2015

Cloud Security Statistics

> "85% of nearly 150 chief information security officers said their organizations are moving to cloud, nearly half expect a major cloud provider to experience a security breach."

- National Institute of Standards and Technology (NIST)

But I love Dropbox…

October 2014 - Hackers got a hold of 7 million Dropbox passwords! The popular cloud storage service denied it has been compromised and that the passwords were taken from **unknown third-party** services. So why did the perpetrators hijack all those passwords? Bitcoin (BTC) digital currency

Be Careful what you Store in the Cloud

May 2014 - Box and Dropbox users unknowingly allowed private data to be read by **third parties** or indexed by search engines.

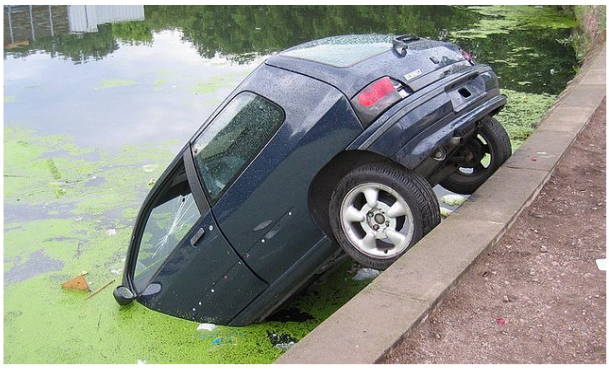
Just ask Code Space

AWS console breach leads to demise of service with "proven" backup plan

Code Spaces closes shop after attackers destroy Amazon-hosted customer data.

by **Dan Goodin** - Jun 18, 2014 4:12pm CDT

Share Tweet 105



Esther Simpson

A code-hosting service that boasted having a full recovery plan has abruptly closed after someone gained unauthorized access to its Amazon Web Service account and deleted most of the customer data there.

June 2014 – Hackers gained access to AWS control panel account – mounted a DDoS attack against Code Space and then systematically deleted all of their machine definitions, all of their data and of course, all of their unprotected backups.

No Client Data
=
No Clients.

A Picture is worth…..?

Aug. 2014 - The Celebrity Photo Leak of 2014 reminded us that our files in the cloud may not be as secure as we initially thought. Shortly after the photos of several celebrities were posted on Reddit, Apple released a statement saying that iCloud was not breached. What are we to do to prevent thieves from accessing our files if/when our passwords are stolen? **Encryption?**

Misconfigurations = Big Headaches!

RESULT - The drive was indexed by Google and it's contents made available to anyone who wanted to access it. Patient data, financial data and some very embarrassing personal pictures were made public.

A user with access to sensitive information purchased a retail external hard drive for extra local storage. The drive was loaded with gigabytes of patient data along with personal photo's and other highly sensitive financial information. Unknowingly, the default configuration for the drive was for it to be **cloud enabled,** so it reached out to the internet to make itself more "convenient" to be accessed from anywhere

Top Cloud Threats

Security Risks	• Data loss in "blind" environment • Co-mingling of private data with other data types • Insufficient due diligence by cloud provider • Shared technology vulnerabilities (Denial of Service attacks) • Data forensics concerns • Immature technology could introduce new risks • Cloud provider audits (on-site and remote) • Poor or no encryption of sensitive data • Account or service hijacking • Client misconfigurations or omission of controls
Compliance	• Application ownership can be unclear • Regulatory controls for cloud (HITECT, PCI, GLBA, FERPA,HIPAA)
Legal/Contracts	• Data "pull-back" at the end of contracts • Lack of SLA's – slow or no service • Lack of recourse for lost data • Jurisdictional issues (data stored across multiple states or countries) • e-Discovery and legal hold issues (data stored across multiple servers) • Use of cloud does not remove the clients responsibilities • Breach notification timeframes

Separating Myth From Fact

Cloud Security Myth #1

Myth: My Cloud Service Provider (CSP) is responsible for the security of my data stored in their environment.

- Fact: Unless specified, most standard CSP agreements place responsibility for data security on the customer – understanding roles and responsibilities is key!

Cloud Security Myth #2

Myth: My CSP encrypts all of my customer data stored on their servers.

Fact: Most CSP offer encryption but as a secondary option and at additional cost. Encryption is one of the single most important security controls you can use to protect sensitive data.

Compliance Myth

Myth: My CSP provides basic security controls (firewall, antivirus, etc.), so I must be compliant with security regulations.

- Fact: Although basic security controls are components of regulatory requirements, additional controls may be required in order to be compliant.

Contracts Myth #1

Myth: I can get my data back and easily move to another vendor anytime I want to.

- Fact: Vendor lock-in is the term associated with issues related to moving your data to another CSP. This can be a real challenge. Data identification, retrieval, clean-up and destruction are all areas of consideration.

Contracts Myth #2

Myth: I contracted with a CSP in the United States, so all of my data will stay in the U.S.

- Fact: Unless specified in your agreement with your CSP, many cloud providers will store your data in a location most beneficial to them. This could include locations outside of the U.S.

Contracts Myth #3

Myth: If there is a breach associated with my data, I will know about right away.

- Fact: CSP's base their response time for breach notification on SLA's or other agreed upon terms. Most standard agreements will state that notification by the CSP can occur up to 30 days following discovery of a breach.

Key Contract Areas

Data termination rights and termination assistance
Performance levels (Service Level Agreements)
Security warranties and problem resolution
Allocation of liability risk
Data Privacy compliance requirements
Data security and breach notification requirements
Compliance with laws and regulations (PCI, HIPAA,GLBA, FERPA)
Forensics in shared environments
Data jurisdictional requirements (keeping data within the U.S)
Change Control – Scheduled and planned interruptions
Subcontracting and Third Parties

Key Contract Areas – cont.

Use of Open Source Software
Application re-development
Security controls for shared environments
The integrity of data stored in the cloud
Assurance of data segregation and isolation
Encryption in transit and in storage (at rest)
Backup and data recovery
Return of data upon termination of the agreement or failure of Cloud Service Provider
The right to audit the entities and the technology
Ownership of intellectual property and Trade-Secret protection

Where Do We Go From Here?

Ask Tough Questions!

- Will my cloud provider be transparent about governance, security and operational issues?
- Will I be considered compliant if I use this CSP?
- Do I know where my data is?
- Will a lack of standards drive unexpected obsolescence?
- Will my provider secure my environment as well as I would?
- Are the hackers waiting for me in the cloud?

Follow the Checklist

- ❑ DO YOUR HOMEWORK !
- ❑ Secure the cloud before procurement – contracts, SLAs, architecture and controls
- ❑ Know provider's third parties, BCP/DR, financial viability, employee vetting process
- ❑ Plan for provider termination & return of assets
- ❑ Identify physical data location when possible

Final Thoughts

- Cloud is here to stay and is a revolutionary technology paradigm shift
- Force a clear understanding of roles and responsibilities to establish trust relationship
- Insist on accountability and transparency from service providers
- Expect to see regulations for tracking and formal disclosure of cloud security incidents
- Cloud Security is a ongoing initiative – it must be reviewed and updated regularly

contact info

Sese Bennett, Senior Manager - CISSP, CISM, QSA, Network+, ITIL
Security and Risk Services
LBMC Information Security
615-309-2420 direct
www.lbmc.com

LBMC INFORMATION SECURITY