Anatomy of a Cloud Computing Data Breach

Sheryl Falk
Mike Olive

ACC Houston Chapter ITPEC Practice Group
September 18, 2014
Agenda

- Cloud 101 – Welcome to Cloud Computing
- Cloud Agreement Considerations
- Responding to a Cloud Data Security Incident
- Cloud- Data Security Tips
Cloud 101
Welcome to Cloud Computing
The Cloud & Cloud Computing

Cloud computing is a model for enabling ubiquitous, 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 is composed of five essential characteristics, three service models, and four deployment models

- NIST Special Publication 800-145, September 2011
The Cloud & Cloud Computing

Cloud Computing = Internet accessing of applications and data stored or running on remote servers controlled by third parties.

Common Features:

- Broad Network Access
- Pooled Resources
- Rapid Provisioning
- Pay as You Go
Cloud Service and Deployment Models

Provider Supplies:
- Applications
- Database
- Middleware
- OS
- Hardware/Networking

Customer provides the rest

Provider Supplies:
- Middleware
- Development Tools
- OS
- Hardware/Networking

Customer provides the rest

Provider Supplies
- Hardware/Networking

Customer provides the rest
Advantages of Cloud Computing

Why Cloud Computing?

- Pay As You Use
- Lower TCO
- Reliability, Scalability & Sustainability
- Secure Storage Management
- Lower Capital Expenditure
- Frees Up Internal Resources
- Highly Automated
- Utility Based
- Easy & Agile Deployment
- Device & Location Independent
- 24X7 Support
Key Considerations
Cloud Contracts/Negotiations
Before Customers Start!

- Why do we want to utilize cloud?
- What applications/data are involved?
  - Assess Criticality.
  - What regulatory/contractual requirements apply?
  - How are we going to move data in/out of the cloud?
- What is our risk tolerance?
1. Data Issues

- Ownership
- Availability
- Security
- Location/Movement/Access
- Compliance with Regulatory Requirements
1.A Data Ownership

Specify **customer ownership** of customer-provided data and data processed/generated in the cloud

- Specify how Supplier may use the data and any permitted third parties disclosures

Provider will want **ownership of database structures** they provide

- Be careful with this at exit
1.B Data Availability

- Include defined service levels for data access and availability.

- Are company data retention requirements specified, including for litigation holds and audit trails?

- Are the parties’ disaster recovery and business continuity obligations and performance goals clearly allocated and stated?

- Specify data backup requirements?
1.C Data Security

- Identify data security requirements in the contract
  - Appropriate for type of data involved
  - Compliant with applicable legal requirements
  - Leverage applicable data security standards (e.g., ISO)
  - Physical and digital security requirements

- Include remedies for data loss, unavailability and/or corruption
  - Service credits
  - Costs to restore or recreate

- Data segregation requirements
1.D  Data Location, Movement, Access

➢ The cloud computing model is inherently cross-border

➢ Specify data location(s)

➢ Customer contractual right to control new locations
  • Are compliant data transfer mechanisms in place (e.g., model contracts, Safe Harbor certification, BCRs, other)?
  • Are flow-down terms required for approved sub-processors?
  • Potential for compelled disclosure to government authorities

➢ What are the provider’s standard practices for responding to subpoenas or other government process? Litigation holds?
1.E Compliance with Regulatory Requirements

- Have customer’s data-related legal compliance requirements been included or referenced in the contract?
- Allocation of responsibility for complying with law changes
- Defined triggers: “security breach”, “security incident”, other?
- Detailed incident response plan, including:
  - Incident verification and notice to customer
  - Customer retains control over notice obligations and communications
- Allocate financial responsibility for breach-related costs
2. Exit Management

What happens upon expiration or termination of agreement?

• Specify the **exit plan and period**.
• No liens or other provider right to withhold data
• Specifications for return of data and **format** requirements
  • Does Customer need use of Provider’s **database structures** in short/long term
• Provider obligation to destroy data securely, at customer’s option
• Provider cooperation with successor
3. The Usual Suspects

- Indemnification
- Liability Caps
- Exclusion of consequential damages
- Provider insurance coverage
4. Other Considerations

- Audit/Subcontracting

- Can either party modify the terms unilaterally?

- Is the customer permitted under law (e.g. export or data privacy) or its other agreements to move data/applications to the cloud and give access to the cloud provider(s)

- Bankruptcy issues

- Consider typical software license issues, particularly for SaaS
Cloud Data Security
How Safe is your data in the cloud?
Cloud Data Breaches
Cloud Computing Top Threats in 2013

① DATA BREACH
② DATA LOSS
③ ACCOUNT OR SERVICE TRAFFIC HIGHJACKING
④ INSECURE INTERFACES AND APIs
⑤ DENIAL OF SERVICE
⑥ MALICIOUS INSIDERS
⑦ ABUSE OF CLOUD SERVICES
⑧ INSUFFICIENT DUE DILLIGENCE
⑨ SHARED TECHNOLOGY VULNERABILITIES
Incident: A security event that compromises the integrity, confidentiality of availability of data

63,437

Breach: An incident that result on the disclosure or potential disclosure of information

1,367
8 Most Common Causes of Data Breaches

1. Weak and Stolen Credentials
2. Back Doors, Application Vulnerabilities
3. Malware
4. Social Engineering
5. Too Many Permissions
6. Insider Threats
7. Physical Attacks
8. Improper User Configuration, User Error

• Information Week: The 8 Most Common Causes of Data Breaches
Cloud Data at Greater Risk of Breach?

Data in the cloud is 3 times more likely to be breached

62% believe that cloud services are not thoroughly vetted

69% believe that their organization is not proactive in assessing information that is too sensitive to be stored in the cloud.
Data Breach Detection

- Less than 2% of breaches are detected in the first 24 hours
- Less than 46% of breaches are detected in the first 30 days
- Over 92% of breaches are discovered by a third party
- 60% of breaches have data exfiltrated in first 24 hours

-- Verizon Data Breach Report
Responding to a Cloud Data Security Incident
Follow your Data Breach Response

- Develop a written Plan
- Assemble your Team
- Identify your Vendor partners
- Test your Plan
The Importance of a Privileged Investigation

➢ Engage Counsel at outset

➢ Direct the forensic/security vendors through counsel

➢ Working with your cloud partner on the investigation

➢ Educate your whole team about Privilege

➢ Be careful what you put in writing
The Data Security Investigation

- Secure the data
- Preserve evidence
- Analyze forensic data
- Interview key witnesses
- Lessons Learned/Remediation
Challenges in a Cloud Investigation

• Control over the Data
• Timely Access to the Data
• Cost of getting the Data
• Access to the Vendor witnesses
• Understanding the Vendor data structure and Security Controls
• Privilege Considerations
Getting to the Heart of the Matter

➢ What type of Information was Involved?
  ▪ Personal information involved?
  ▪ Payment Card Information
  ▪ Health Information
  ▪ Confidential, trade secret data involved?

➢ How was the information protected? (Encryption)

➢ Was the data actually compromised?
What are your obligations?

- Federal or State Laws may require action
  - Depends type of information at issue
  - Depends on threshold numbers affected
  - SEC Report Requirement if “material breach”

- Impacted individuals
  - Applicable law is where individual resides
  - Legal implications of failing to properly notify
Texas Data Breach Statute

521.053 Texas Bus. & Com. Code

“A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach…to any individual whose sensitive personal information…believed to have been acquired by an unauthorized person.”

- Extraterritorial Application
- Civil penalty up to $250,000 per breach
47 State Notification Laws

- The trigger for notification
- Who to notify
- Timing of notification
- Contents of notice
- Methods for providing notice
If Laws Impacted, Notice Will Be Needed

- Impacted individuals
- Government Authorities
- Credit reporting agencies
- Contractual Partners
- Press

If Laws Impacted, Notice Will Be Needed.
What Notices Look Like

- Describe incident
- Categories of information
- Consequences of breach/nature of risk
- Protection measures put in place
- Advice about how to protect self
Does the Company Have a PR Strategy Ready?

- What happened?
- When did it happen?
- What information was compromised?
- Was my information compromised?
- How many people’s information was impacted?
- Was the information encrypted?
- Was my social security number compromised?
- Did anyone misuse this information?
- What should I do?
- What are you doing to protect me?
- Will this happen again?
- Who should I contact if I have more questions?
Responding to the AG/Regulators

- Maintain your credibility
- Negotiate terms of requests
- Circulate a hold for document destruction
- Advocate your story
After Action Event Review

- How did the team respond?
- What can be improved in response/investigation?
- What security issues can be tightened up?
- Modify your plan/procedures if necessary
Cloud Data Security Measures
Conduct Effective Due Diligence

- Right to Audit
- Obtain Data Security Controls data
- Industry certifications, third party assessments, audits
- Shared environment security
- Logging and monitoring capabilities
- Use of subcontractors for data-related processes
- Data transfer/transition policies
- Data recoverability and data destruction practices
Tips for Securing your data in the Cloud

1. Classify what data needs to be protected
2. Protect your most sensitive data
   • Encrypt your sensitive data
   • Tokenization
   • Data loss prevention systems
3. Consider multi-factor authentication
4. Enforce lock out policies
5. Keep good logs and have a process to review
6. Pro-actively investigate suspicious activity
Get Serious About Password Management

- Educating users about how to select passwords
- Minimum Password Length – 13 Characters or more
- Complexity Requirements
- Enforce Password History
- Use Maximum Password Age
- Be Careful about shared-use Process or Admin passwords.
Course No. 901295791

Questions?
Sheryl Falk
713.651.2615
sfalk@winston.com

Mike Olive
Managing Counsel
BP Legal