NETSECURE'11

IT SECURITY & FORENSICS CONFERENCE & EXPO • MARCH 24-25, 2011 - WHEATON, IL

Negotiating Contracts That Will Keep our Clouds Afloat:

You're going to put THAT in a cloud?

Meteorologist: Daniel T. Graham

CLARK HILL

What is Cloud Computing?

- "The dynamic provisioning of IT capabilities, whether hardware, software, or services from a third party over the network" *– Accenture, 2009*
- Cloud computing may be viewed as "outsourcing" of these capabilities.
- Maintaining control over the unpredictability of the forecast.
  - *Should you stay indoors or venture out*?

Cloud Computing Forecast: Sunny Skies with Contract Must Haves

1. Security	2. Performance	3. Audit	4. Remediation	5. Mobility
⛈	🌧	☁	⛅	☀

Security

- First, consider the criticality of software, data, or services in question:
  - **Non-core business** tools or routine, non-sensitive data?
    - Might make sense for looser contract terms, low cost
  - **Mission critical systems**, regulated personal data, or sensitive business intelligence?
    - Data ownership/security issues must be specified in contract
      - Failure to do so could expose you to serious violations of applicable privacy and export laws
      - Examples: private cloud, data encryption, geographic restrictions

Security

- Data should be replicated and continuously updated to be unaffected by outages or disasters
- Vendor should provide real-time data streams from intrusion detection systems
  - If vendor has any kind of breach in its cloud, you should immediately receive notification
- Vendor's obligations should be specified in the event of a virus, hacking or denial of service attacks

7 Security Issues to Consider for Cloud Contracts:

1. Privileged User Access
2. Regulatory Compliance - Confidentiality
3. Data Location
4. Data Segregation
5. Recovery
6. Investigative Support
7. Long-Term Viability - Transition

- Gartner, 2008

Security

1. Privileged User Access –
    - Get as much info as you can about the people who manage your data – are they all “in-house”?
    - Hiring and oversight of privileged administrators and the controls over their access
2. Regulatory Compliance –
    - Vendor should comply with audits and security certifications. Is it SAS 70 / ISO 27001 certified?
    - Are you licensing vendor software? Do you have permission to use?

Security

3. Data Location –

- Private cloud? Is the vendor merely a subcontractor?
- Ask provider to commit to storing and processing data in specific jurisdictions
- Contractual commitments to obey local privacy laws

4. Data Segregation –

- Vendor should provide evidence that encryption schemes are in place and tested

5. Recovery –

- Vendor should have ability to do complete restoration in case of disaster

Security

6. Investigative Support –

- Cloud services can be especially difficult to investigate
  - Logging and data for multiple customers may be co-located and/or spread across an ever-changing set of hosts and data centers.
  - Vendor should give you a contractual commitment to support specific forms of investigation.
  - **E-discovery** may be important. If subpoenaed, how do I get the information to comply with the Court's order?

7. Long-Term Viability – Transfer of Data

- Verify that data will be transferred in the event your provider ceases to exist, is acquired or contract ends.

Performance

- Seek a balance between importance of cloud resources and what you can afford for performance premiums
- Change Management processes to be described
- Service level requirements, performance metrics and thresholds should be stipulated in contract for business continuity:
  - Average application response times, transactions per second, monthly downtime figures, vendor help desk support response time, hardware and software maintenance

Performance

- Ask for customer references to gauge vendor’s performance record
- *Contract Example*: City of Los Angeles’ Google services contract limits downtime to no more than 5 minutes per month before stiff penalties kick in for the vendor
- Set performance goals and clawback of fees if performance standards are not met.
- Is pricing clear? Based on usage or load, or both?

Performance

- **SLA -** *Downtime Severity Levels I-III*: Define them so that you can understand what and when solutions will be offered in the event of:

  I. Halt in Business

  II. Business impacted, but workaround

  III. Non-critical

- **Set Performance Standards**:
  - Availability based on written criteria: the “9’s”. Example: 99.9 % equates to 40 minutes down/month.

Audit

- Demand transparency!
- Actively monitor your vendor’s performance for glitches
- Vendors should document system uptime and processing rates via monthly reports or electronic dashboards

Audit

- Vendor should authorize customer to audit its electronic and physical security practices:
  - On-site visits, interviews with employees
    - Ask questions about the qualifications of vendors’ architects, coders, operators
  - Confirm vendor’s risk-control processes, level of testing done to verify service is functioning as intended, and that vendor can identify vulnerabilities
  - These audits are essential as the cloud becomes a part of customer’s functional data center under government security regulations

Remediation

- Avoid contracts that lack consequences for vendors that don’t meet their contractual obligation
  - Be wary of a vendor who agrees to everything
    - If penalty for failing to deliver is insignificant, can be cheaper for vendor to fail than to follow through
- Breakdowns like excessive downtime should incur monetary penalties
  - *Examples*: refund for a portion of your service fees, service credits or days of free service added

Remediation

- *Security violations* should incur more serious consequences: termination/exit rights if provider fails to notify of security breach
- *"As is" warranties?* What is the vendor proposing it will do if there is a problem?
- *Dispute Resolution procedures* – define them
- *Contract Example*: Los Angeles/Google apps contract entitles Los Angeles to minimum award of $10,000 if any data compromised with power to seek unlimited damages if violation egregious.

Mobility

- Lack of data compatibility standards can make it difficult to move data/applications from one provider to another
  - **Contract should explicitly provide that you remain the sole owner of your data**, no matter where it physically resides
  - You should have ready and unlimited access to data
  - You should have the right to get data back at any time
  - You should be able to get data back without restrictions upon termination of agreement → contract should have provision requiring vendor **to provide termination assistance** when contract ends

Mobility

- Movement of data may involve transfer from servers in one jurisdiction to servers in another
  - Could invoke different jurisdictional-dependent discovery rules, privacy laws and data-transfer restrictions
    - You may want to restrict/prohibit relocation of data to avoid exposure
  - Overseas data storage can pose entirely different set of risks – EU standards are higher than US’s

CLARK HILL

Mobility

- *Contract Example:* Los Angeles/Google apps contract requires LA to receive its full storehouse of data within 5 days of request and data moved to any location of LA’s choosing, including alternative vendor; data must also exist as standard format that wouldn’t incur added costs to LA to store in environment other than Google’s

How to Avoid Stormy Weather with Cloud Contracts

- Don’t assume contract provides adequate customer data protection
  - Ask tough questions!
  - Consider getting a security or risk assessment from a neutral third party before committing to a cloud service provider
- Don’t assume there’s no room to negotiate even with boilerplate contracts

Cloud Disasters & Successes

- Heartland Payment Systems 2007 security breach of Visa card issuers' info → settlements of $65+ million

vs.

- City of Los Angeles & CSC's customized, five year contract of Google apps

Cloud Successes…

Today's Forecast:

Is bright and sunny,

with an 80% chance that I'm wrong.

Thanks for tuning in.

Daniel T. Graham

Clark Hill PLC

150 North Michigan Avenue
Suite 2700
Chicago, Illinois 60601
dgraham@clarkhill.com
312.985.5945