REGIONAL FORUMS for SENIOR IT LEADERS

CIO PERSPECTIVES

Produced by

CIO

In partnership with

CIO Executive Council
Leaders Shaping the Future of Business

CIO
PERSPECTIVES

When the Cloud Turns Toxic
A CIO's Guide to Managing Risk

Matt Karlyn

Partner

Foley & Lardner LLP

(617) 502-3231

mkarlyn@foley.com

CIO PERSPECTIVES

Can Maryfran predict the future?

As the siren song of cloud computing grows ever-more enticing to companies of all sizes, it's easy to overlook the kind of risks that keep lawyers awake at night. "What could go wrong?" asks Matt Karlyn, a partner at Foley & Lardner LLP. ***"Well, one day you wake up and see the news that your supplier just suffered a breach and it was all your data." (emphasis added)***. Taking a tough look at the toxic aspects of cloud, Matt will cover the key risks that every company should evaluate before signing any deal for cloud-based services. He'll delve into the ideal contract language to look for, the importance of maintaining control and ownership of the data and the best questions to ask about security.

CIO PERSPECTIVES

The Toxic Cloud…

HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS

Subscribe to The Times

The New York Times

Business Day
Technology

Search All NYTimes.com

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION | ARTS | STYLE | TRAVEL | JOBS

Search Technology
Go

Inside Technology
Internet | Start-Ups | Business Computing | Companies

Bits Blog »

Personal Tech »
Digital Cameras | Cellphone

Advertise on NYTim

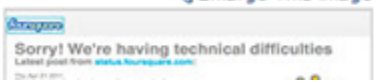
Amazon's Trouble Raises Cloud Computing Doubts

By STEVE LOHR
Published: April 22, 2011

As technical problems interrupted computer services provided by Amazon for a second day on Friday, industry analysts said the troubles would prompt many companies to reconsider relying on remote computers beyond their control.

SIGN IN TO E-MAIL
PRINT
REPRINTS

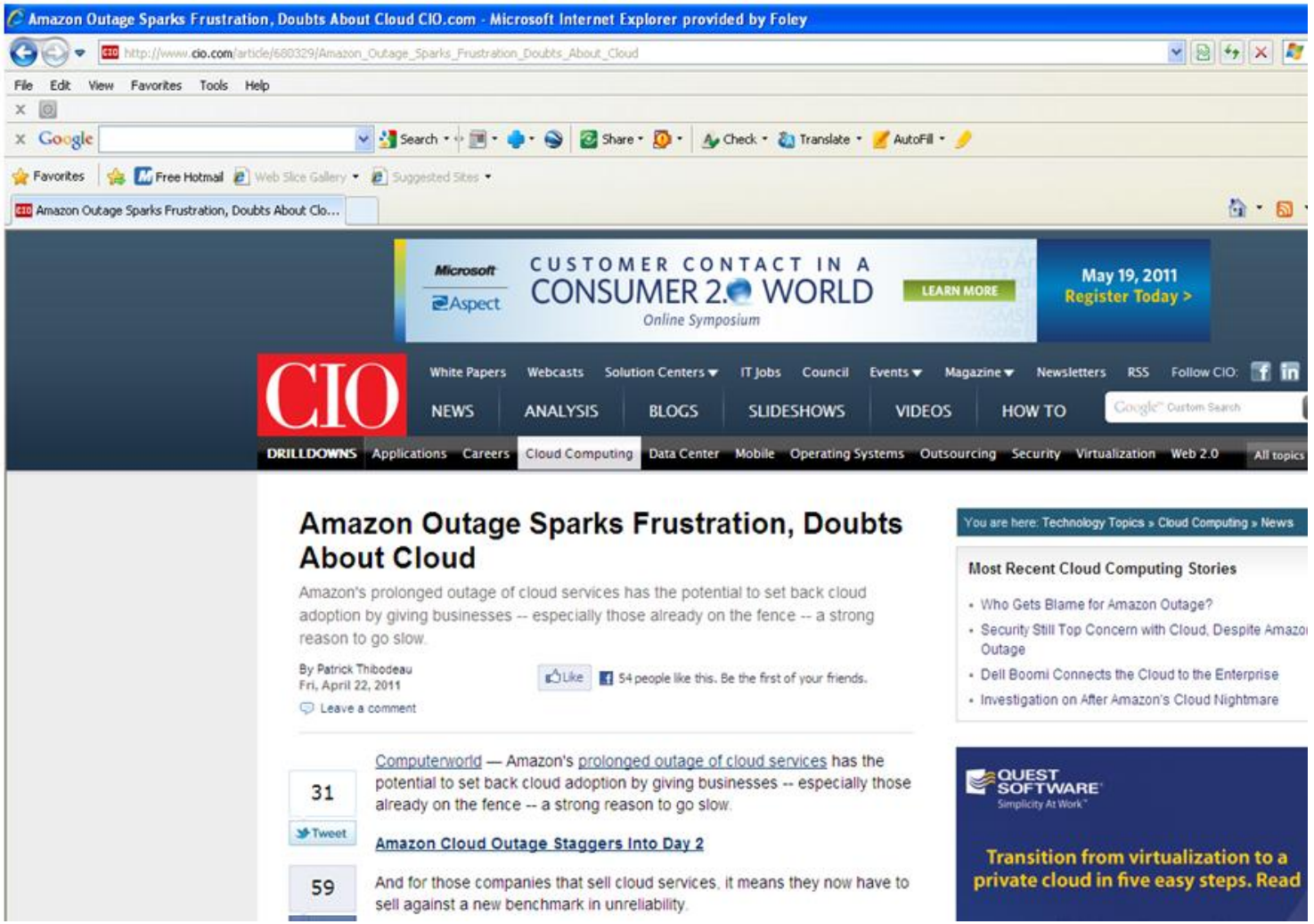
Enlarge This Image



"This is a wake-up call for cloud computing," said Matthew Eastwood, an analyst for the research firm IDC,

CIO
PERSPECTIVES

The Toxic Cloud…



CIO PERSPECTIVES

"A Wake Up Call for Cloud Computing"*

- What you send to the cloud and what you manage on-site
- Backup and recovery services
- Geographic dispersion of data centers
- Impact
  - Distrust of suppliers -- failure to communicate with customers
  - Slower adoption rates
  - In-house solutions
  - Infrastructure investments
  - "The sad irony is that Amazon will emerge from this much better."
    - Tref Laplante, CEO of WorkXpress, Amazon Outage Sparks Frustration, Doubts About Cloud, Computerworld, April 22, 2011

*Matthew Eastwood, IDC, in April 22, 2011 New York Times article, "Amazon's Trouble Raises Cloud Computing Doubts."

CIO PERSPECTIVES

What they are saying…

- Inability to access data, service interruptions, sites being shut down
  - Results in:
    - lost revenue, loss of customers, vulnerability of data
- "The Amazon interruption…was the computing equivalent of an airplane crash." Lew Moorman, Chief Strategy Officer of Rackspace (a specialist in data center services)
- "And for those companies selling cloud services, it means they now have to sell against a new benchmark in *unreliability* (emphasis added."
    - Amazon Outage Sparks Frustration, Doubts About Cloud, Computerworld, April 22, 2011
- "For some, the Amazon outage may reinforce beliefs that cloud services aren't ready for businesses."
    - Amazon Outage Sparks Frustration, Doubts About Cloud, Computerworld, April 22, 2011

CIO PERSPECTIVES

Top Technology With Enormous Growth

- The Top 10 Technologies for 2011
  - #1 – Cloud Computing
- From IDC – "Corporate cloud computing is expected to grow rapidly, by more than 25% a year, to $55.5 billion by 2014

"Amazon's Trouble Raises Cloud Computing Doubts," New York Times, April 22, 2011

CIO PERSPECTIVES

We already know what cloud computing is…

- Delivery over the Internet (i.e., the "cloud")
- Software, platform or infrastructure resources provided as services
- Scalability on-demand
- Utility and/or subscription billing (i.e., based on the customer's actual use and/or a period of time)

CIO PERSPECTIVES

Scalability-on-Demand

- IT resources are “scaled” up or down based on the customer’s demands
  - Scalability → ability to scale up to “unlimited” resources
  - Elasticity → ability to quickly add and remove resources (within seconds or minutes, as opposed to days or weeks, or not at all)
- Economies of scale in the cloud through
  - Virtualization
  - Multi-tenant software architecture

CIO PERSPECTIVES

Utility / Subscription Billing

- Utility billing → payment is based on the amount of resources used, similar to how a person is charged for water, gas, electricity
  - e.g., per virtualized machine each hour; per gigabyte of storage each month; per active user each month
- Subscription billing → payment is based on a period of time, similar to how a person is charged for a newspaper or magazine subscription (e.g., per month)

CIO PERSPECTIVES

Benefits of the Cloud

- Cost reduction
- Service flexibility
  - Quickly set up and implement an IT solution
  - Access IT services anywhere any time Internet
  - Ability to add and remove IT resources on-demand so that customers can effectively and efficiently respond to internal business requirements and changing market conditions
- Lower upfront risks and complexity with realizing the benefits of new technology
- Reduction in capital costs

CIO
PERSPECTIVES

That all sounds great …

CIO PERSPECTIVES

Data Sensitivity and the Criticality of the Service

- High Risk = mission critical processes utilizing highly sensitive data
- Medium Risk = generally available data that requires high service levels; non-confidential enterprise data
- Low Risk = not mission critical and generally available data; can accept outages and variable performance

- *Solutions must be carefully evaluated to ensure the benefits outweigh the risks; ensure contractual protections and operational precautions are taken*

CIO PERSPECTIVES

Speaking of Contracts…

- *But another issue, Mr. Eastwood said, will be the re-examination of the contracts that cover cloud service…"*

"Amazon's Trouble Raises Cloud Computing Doubts," New York Times, April 22, 2011

CIO PERSPECTIVES

Licensing vs. the Cloud

- Cloud computing agreements have *some* similarity to licensing agreements, but have more in common with hosting or ASP agreements
- Traditional licensing/hardware purchase
  - Vendor installs the software or equipment in the customer's environment
  - Customer has ability to have the software or hardware configured to meet its needs
  - Customer retains control of the data
- In the cloud…
  - Software, hardware and customer data are hosted by the provider typically in a shared environment (e.g., many customers per server)
  - Software and hardware configuration much more homogeneous across all customers
- Shift of top priorities
  - From configuration, implementation and acceptance (in the licensing world) to service availability, performance, service levels, data security and control (in the cloud)
- Traditional provisions do retain importance
  - E.g., → insurance, indemnity, intellectual property, limitations of liability, warranties

CIO PERSPECTIVES

Cloud Customers Must Make Important Decisions

- There are no standard forms that work for every customer, for every product, in every deal
  - Some commonly used outsourcing and software licensing terms may be useful, but cannot be uniformly applied to cloud computing transactions
- More robust contractual protection and provisions that address issues unique to the cloud are likely needed
  - For the “low risk” deals, a low risk solution may outweigh the need for contractual protections
  - For “high risk” deals, better to take a closer look and include the provisions that will protect your company
  - Note that robust contractual protections may have an impact on price and eliminate certain providers altogether

CIO PERSPECTIVES

The Focus of Cloud Computing Transactions

- Focus should be on:
  - The criticality of the software, data and services to the enterprise
  - The unique issues presented by a cloud computing environment
  - The service levels and pricing offered by different suppliers and for different services
  - Outsourcing agreements and traditional licensing agreements are a good starting point, but not a good ending point

CIO PERSPECTIVES

A Brief Disclaimer…

- Note that these slides and this presentation contain several examples of language that is commonly found in cloud computing agreements. These slides and this presentation are not a substitute for legal advice. The language to be used in your transactions depends on a variety of factors and the particular circumstances. You are strongly advised to engage knowledgeable legal counsel to access and help minimize your legal liabilities based on the particular requirements of your organization. Like any presentation or article, this is not meant to be a substitute for knowledgeable legal counsel.

CIO PERSPECTIVES

Pre-Agreement Due Diligence

- Can the provider meet your company's expectations?
- Require provider to complete a due diligence questionnaire
  - Provider's financial condition
  - Insurance
  - Existing service levels
  - Capacity
  - Physical and logical security
  - Disaster recovery and business continuity
  - Redundancy
  - Ability to comply with applicable regulations

CIO PERSPECTIVES

Service Availability

- If the provider stops delivering services, the customer will have no access to the services (which may be supporting a critical business function), and perhaps more importantly, no access to the customer's data stored on the provider's systems
- A customer must be able to continue to operate its business and have access to its data at all times

CIO PERSPECTIVES

Service Availability

- What do you need?
  - An appropriate uptime service level
  - Data ownership rights and the provider's commitment to perform regular full and partial data backups
  - Disaster recovery and business continuity assurances
    - ***For example, "Provider shall maintain and implement disaster recovery and avoidance procedures to ensure that the Services are not interrupted during any disaster. Provider shall provide Customer with a copy of its current disaster recovery plan and all updates thereto during the Term. All requirements of this Agreement, including those relating to security, personnel due diligence, and training shall apply to the Provider disaster recovery site."***
  - Provider's agreement not to withhold services (even if there is a dispute)
    - ***For example, "Provided Customer continues to timely make all undisputed payments, Provider warrants that during the Term of this Agreement it will not withhold services provided hereunder, for any reason, including, but not limited to, a dispute arising under this Agreement, except as may be specifically authorized herein."***
  - Protections against provider's financial instability
    - ***For example, "Quarterly, during the Term, Provider shall provide Customer with all information reasonably requested by Customer to assess the overall financial strength and viability of Provider and Provider's ability to fully perform its obligations under this Agreement. In the event Customer concludes that Provider does not have the financial wherewithal to fully perform as required hereunder, Customer may terminate this Agreement without further obligation or liability by providing written notice to Provider."***

CIO PERSPECTIVES

Service Levels

- Other common service level issues that customers should address are:
  - Performance and responsiveness of the services
    - Avoid services that are effectively unavailable
  - Simultaneous visitors
  - Problem response time and resolution time
  - Data return and periodic delivery
  - Remedies for failure to meet service levels

CIO PERSPECTIVES

Service Levels

- Why are they so important?
  - Assure the customer that it can rely on the services in its business and provide appropriate remedies if the provider fails to meet the agreed service levels
  - Provide agreed upon benchmarks that facilitate the provider's continuous quality improvement processes and provide incentives that encourage the provider to be diligent in addressing issues

CIO PERSPECTIVES

Service Levels

- Uptime – an example
  - ***For example, "Provider will make the Services Available continuously, as measured over the course of each <u>calendar month</u> period, an average of <u>99.99%</u> of the time, excluding unavailability as a result of Exceptions (as defined below) (the "Availability Percentage"). "Available" means the Services shall be available for access and use by Customer. For purposes of calculating the Availability Percentage, the following are "Exceptions" to the service level requirement, and the Services shall not be considered un-Available if any inaccessibility is due to: (i) Customer's acts or omissions; (ii) Customer's Internet connectivity; or (iii) Provider's <u>regularly scheduled downtime</u> (which shall occur weekly, Sundays from 2:00 a.m. to 4:00 a.m. eastern time).***

CIO PERSPECTIVES

Service Levels

- Response Time – an example
  - Maximum latencies and response times for the customer's use of the services
    - ***For example, "The average download time for each page of the Services, including all content contained therein, shall be within the lesser of (i) 0.5 seconds of the weekly Keynote Business 40 Internet Performance Index ("KB40"), or (ii) two (2) seconds. In the event the KB40 is discontinued, a successor index (such as average download times for all other customers of Provider) may be mutually agreed upon by the parties."***

CIO PERSPECTIVES

Service Levels

- Remedies – an example
  - ***For example, "In the event the Services are not Available 99.99% of the time, but are Available at least 95% of the time, then in addition to any other remedies available under this Agreement or applicable law, Customer shall be entitled to a credit in the amount of $____ each month this service level is not satisfied. In the event the Services are not Available at least 95% of the time, then in addition to any other remedies available under this Agreement or applicable law, Customer shall be entitled to a credit in the amount of $____ each month this service level is not satisfied. Additionally, in the event the Services are not Available 99.99% for (i) three (3) months consecutively, or (ii) any three (3) months during a consecutive six (6) month period, the, in addition to all other remedies available to Customer, Customer shall be entitled to terminate this Agreement upon written notice to Provider with no further liability, expense, or obligation to Provider."***

CIO PERSPECTIVES

Data – Security, Redundancy, Ownership and Use Rights, Conversion

- The security of a customer's data in a cloud computing environment has been recognized as one of the largest areas of concern for a customer
  - The customer is ultimately responsible for complying with privacy and security regulations, and data security breaches are costly
- To confirm it is able to continue using its data, the customer should confirm ownership of all data stored by the provider
  - Require regular backups
  - Require appropriate data conversion
- Require provider to maintain confidentiality of data
- Place appropriate limitations on the provider's ability to use the data and customer information

CIO PERSPECTIVES

Data – Security, Redundancy, Ownership and Use Rights, Conversion

- Increased risk of unauthorized disclosure
  - Multi-tenancy in the cloud – your data may be stored on a server with other customer's data = increased risk of unauthorized disclosure

CIO PERSPECTIVES

Data – Security, Redundancy, Ownership and Use Rights, Conversion

- Due diligence is important
  - Where is the data going to be located?
- Who will have access to the data?
- Will offshore be permitted?
  - Which law governs?
- Who is operating the data center – the provider or a third party?
  - Ensure third party hosts comply with your agreement
  - Provider should accept all responsibility for the third party host
  - Provider should be jointly and severally liable with the third party host for any breach of the agreement by the third party host
  - Consider entering a separate confidentiality agreement with the third party host
  - Advance notice if any change of the host

CIO PERSPECTIVES

Data – Security, Redundancy, Ownership and Use Rights, Conversion

- Providers should be required to provide:
  - Baseline security measures
  - Security incident management
  - Hardware, software and security policies
- Some providers won't show you their security policies but will permit onsite access to them
  - You should go and review them
- Ensure that these policies address security issues particular to cloud computing and services being provided over the internet

CIO PERSPECTIVES

Data – Security, Redundancy, Ownership and Use Rights, Conversion

- Provider must notify the customer in the event it is required by law to disclose your company's data
  - Written notice sufficiently in advance
  - Reasonable efforts not to release data pending the outcome of any measures taken by your company to oppose the required disclosure

CIO PERSPECTIVES

Data – Security, Redundancy, Ownership and Use Rights, Conversion

- In the event of a security breach:
  - Customer has sole control over the timing, content, and method of customer notification (if it is required)
  - If the provider is responsible for the breach, then the provider must reimburse the customer for its reasonable out-of-pocket expenses in providing the notification and otherwise complying with the law

CIO PERSPECTIVES

Data – Security, Redundancy, Ownership and Use Rights, Conversion

- For example
  - ***"a. In General. Provider will maintain and enforce safety and physical security procedures with respect to its access and maintenance of Customer Information (i) that are at least equal to industry standards for such types of locations, (ii) that are in accordance with reasonable Customer security requirements, and (iii) which provide reasonably appropriate technical and organizational safeguards against accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access of Customer Information and all other data owned by Customer and accessible by Provider under this Agreement.***
  - ***b. Storage of Customer Information. All Customer Information must be stored in a physically and logically secure environment that protects it from unauthorized access, modification, theft, misuse, and destruction. In addition to the general standards set forth above, Provider will maintain an adequate level of physical security controls over its facility. Further, Provider will maintain an adequate level of data security controls. See Exhibit A (Security Policies) for detailed information on Provider's security policy protections.***
  - ***c. Security Audits. During the Term, Customer or its third party designee may, but is not obligated to, perform audits of the Provider environment, including unannounced penetration and security tests, as it relates to the receipt, maintenance, use, or retention of Customer Information. Any of Customer's regulators shall have the same right upon request. Provider agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits with reasonable timeframes."***

CIO PERSPECTIVES

Fees

- Ability to add and remove resources with a corresponding upward or downward adjustment in the service fees
- Identify all potential revenue streams and make sure that the identified fees are inclusive of such revenue streams
- Lock in recurring fees for a period of time (one to three years) and thereafter an escalator based on CPI or another index

CIO PERSPECTIVES

Term

- The customer should be able to terminate the agreement at any time upon notice (14 to 30 days) and without penalty
  - The software and infrastructure are being provided as a service and should be treated as such
  - The provider may request a minimum commitment from the customer to recoup the provider's "investment" in securing the customer as a customer
    - If you agree to this, limit to no more than one year and the provider should be required to provide evidence of its up front costs to justify such a requirement

CIO PERSPECTIVES

Indemnification

- Third party claims relating to the provider's breach of its confidentiality and security obligations, and claims relating to infringement of third party intellectual property rights
  - Limitation to copyright is not acceptable
  - Limitation to US IP rights may be acceptable, but consider whether use of the services will occur overseas

CIO PERSPECTIVES

Limitation of Liability

- Scrutinize limitation of liability provisions carefully
- If you can't eliminate the limitation of liability in its entirety, seek the following protections:
  - Mutual protection
  - Appropriate carve-outs (e.g., confidentiality, data security, indemnity)
  - A reasonable liability cap for direct damages

CIO PERSPECTIVES

Warranties

- The following warranties are common in these types of agreements:
  - Conformance to specifications
  - Performance of services
  - Appropriate training
  - Compliance with laws
  - No sharing / disclosure of data
  - Services will not infringe
  - No viruses / destructive programs
  - No pending or threatened litigation
  - Sufficient authority to enter into agreement

CIO PERSPECTIVES

Insurance

- Customer should self-insure against IT risks by obtaining a cyber-liability policy
- Provider should be required to carry:
  - Technology errors and omissions liability insurance
  - Commercial blanket bond, using Electronic & Computer Crime or Unauthorized Computer Access insurance
- Most data privacy and security laws will hold the customer liable for security breaches whether it was the customer's fault or the provider's fault

CIO PERSPECTIVES

Exclusivity

- In order for customers to obtain the best pricing, providers are asking customer to contractually commit to an exclusive arrangement
- Before entering into such an arrangement, ensure your company has the proper protections in the agreement
  - Excellent service levels
  - Appropriate exceptions to exclusivity
  - Right to transition in anticipation of termination
- You don't want to be bound to a poorly performing provider!
- Weigh pricing advantages with performance commitments and reliability of the provider

CIO PERSPECTIVES

Post-Execution Ongoing Provider Assessment

- Regular program of evaluating a provider's performance
  - Provider required to supply the requisite information to access the services
  - Notify the customer of any changes with regard to the provider
  - Provide recommendations to improve the services

CIO PERSPECTIVES

Negotiation

- Leverage is important – you may not be able to obtain all of the protections you want
- Evaluate the business risks
  - Do the services support a critical business function?
  - Do the services involve sensitive data?
  - Are the services customer facing?
- If you can't get the protections you want in the most significant areas of risk, consider walking away
- If walking away is not an acceptable option, focus on risk mitigation
  - For example, if the provider refuses to modify its uptime service level (arguing that it cannot separately administer an uptime warranty for different customers) focus on improved remedies and exit rights for failure to meet the service level

CIO PERSPECTIVES

Part 4 -- Additional Provisions to Consider

- Ability to audit
- Lack of transparency and control
- Subcontracting and flow down of provisions
- IP issues
- Change management and governance/oversight

CIO PERSPECTIVES

QUESTIONS?

Matt Karlyn

Partner

Foley & Lardner LLP

mkarlyn@foley.com

(617) 502-3231