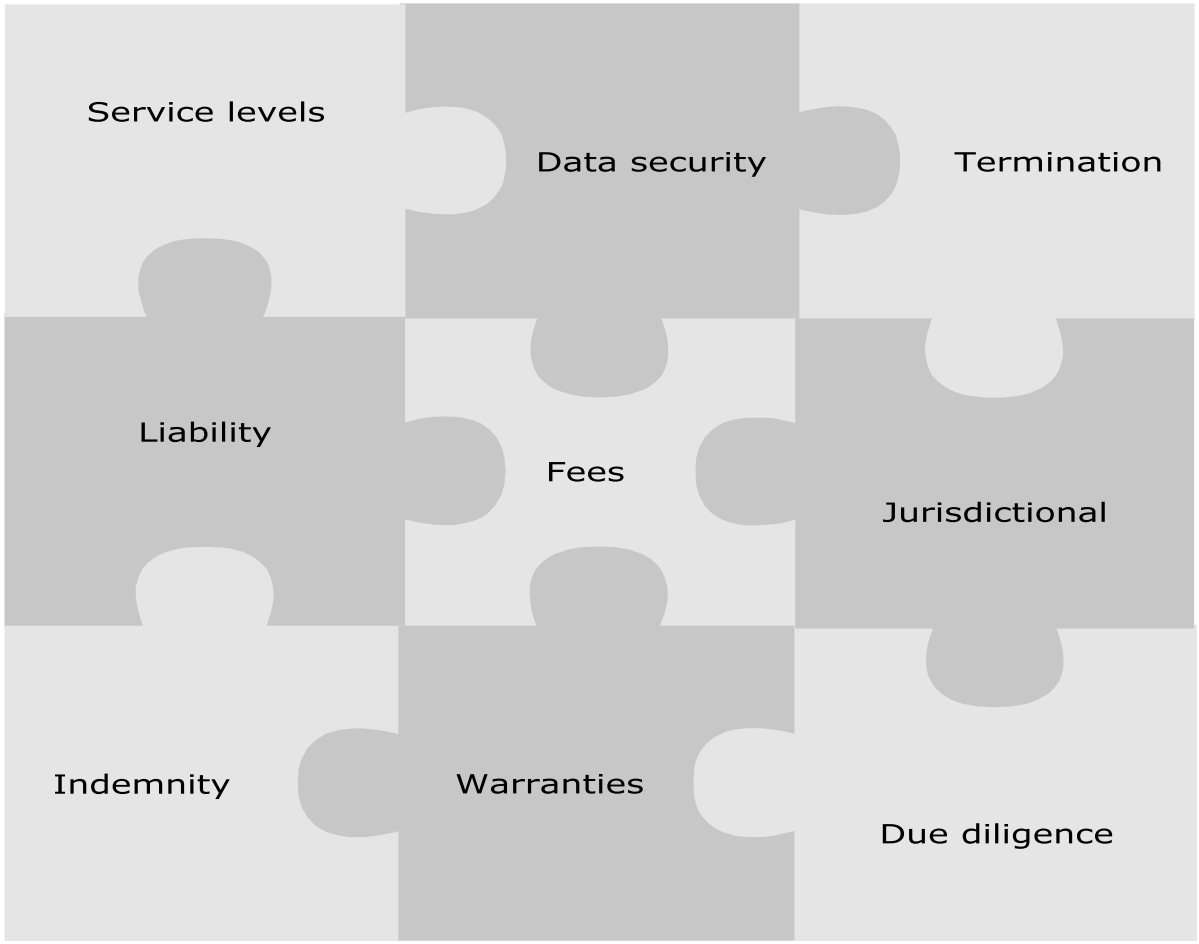
Securing the Cloud: What You Should Be Worrying About, and Why

Michael Overly, Esq., CISA, CISSP, CIPP, ISSMP, CRISC

Partner

Foley & Lardner LLP

Legal Challenges of the Cloud



Vendor Contract Protections Not Optional

- Security protections in vendor agreements are required by law:
  - GLB
  - HIPAA/HITECH
  - Massachusetts, California, Maryland, etc.
  - FACTA

Security Best Practices: ISO

- ISO 27001 and ISO 27002/17799: "Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements."

CERT Resiliency Management Model

- Manage operational risk, includes three fundamental activities: Security, business continuity and IT operations.
- Managing relationships with business partners to achieve operational resiliency
  - Due diligence
  - Contractual obligations

CERT Definition of "Insider"

- Last year, CERT identified 100+ significant incidents of "insider" breaches.
- CERT recently modified its official definition of "insider" from "current and former employees" to "current and former employees, business partners and contractors."

FFIEC: Outsourcing Technology Services

- Federal Financial Institutions Examination Council
- IT Examination Handbook assists financial institutions and examiners in evaluating risk management in IT relationships
  - Due diligence
  - Vendor contracting standards
- Excellent reference for every business

Three Step Approach

- ✓ Vendor due diligence
- ✓ Contractual protections
- ✓ Information handling procedures and requirements, generally in the form of contract exhibits

Service Availability

- Provider may stop delivering services to client, due to:
  - a server being down,
  - failure of a telecommunications link,
  - a natural disaster causing damage to the provider's data center,
  - provider withholding services because of a fee dispute, or
  - provider closing its business because of financial difficulties
- Result:
  - Client has no access to
    - the services (which may be supporting a critical business function), and
    - any client data stored on the provider's systems

Service Availability

- Client needs to be able to
  - continue to operate its business, and
  - have access to its data at all times.

- The proper contractual protections are needed to address the various risks relating to service availability

Service Availability – Service Levels

Scenario: Server is down, or failure of a telecommunications link

- Include uptime service level to ensure service availability is aligned with the client's expectations
- Also, include appropriate remedies to incentivize provider to perform in accordance with service levels
- Uptime service level and the corresponding remedies discussed in more detail in later slides

Service Availability – Disaster Recovery and Business Continuity

Scenario: Natural disaster is causing damage to the provider's data center

- Include a provision requiring the provider to continue to make the services available, even in the event of a disaster, power outage, or similarly significant event.
  - Continuity of services should be provided through a secondary server, data center, or provider, as appropriate.
- Review any related provider policies and procedures
- 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 Client 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.

Service Availability – Withholding of Services

Scenario: Provider is withholding service because of a fee dispute

- Include a provision prohibiting the provider's withholding of services
- Example:

Provided Client 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 between the parties arising under this Agreement, except as may be specifically authorized herein.

Service Availability – Bankruptcy; Financial Wherewithal

Scenario: Provider is closing its business because of financial difficulties

- Include a bankruptcy provision
  - provides the client the right to terminate the Agreement in the event of a provider bankruptcy
- Include a transition assistance services provision
  - requires the provider to assist in transition of the services to a 3rd party provider or to the client, in the event of expiration or termination of the Agreement
- However, once the provider has declared bankruptcy, Provider's ability to assist the client may be limited

Service Availability – Bankruptcy; Financial Wherewithal (cont'd.)

Scenario: Provider is closing its business because of financial difficulties

- If the client is not confident of the provider's financial stability, then consider adding a provision that enables the client to identify provider's financial issues *in advance*
  - Require the provider to deliver periodic reports on its financial condition

- Example:

Quarterly, during the Term, Provider shall provide Client with all information reasonably requested by Client 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 Client concludes that Provider does not have the financial wherewithal to fully perform as required hereunder, Client may terminate this Agreement without further obligation or liability by providing written notice to Provider.

Service Availability – In-House Software Solution

- If provider stops providing “infrastructure” services …
  - client may be able to switch to another 3rd party provider or purchase the required equipment to replace
- However, if provider stops providing “software” services …
  - “software” services may be unique and more difficult to replace
- Consider requiring the provider to make available or develop an in-house solution
  - Inclusion of this provision is very dependent on the nature of the software provided as a service
  - the more critical the application, the more important it is to require provider to develop a long term in-house solution

Service Availability – Client Data

- Explicitly specify client's ownership of any information stored by the provider for the client

- Require that provider
  - deliver periodic copies of all client data to client, and
  - perform regular data backups to an off-site storage facility

Service Levels

- Most common service level issues:
  - uptime
  - service response time
  - problem response time and resolution time
  - data return
  - remedies
- Two main purposes:
  - assure the client 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 process and provide incentives that encourage the provider to be diligent in addressing issues

Service Levels – Uptime Service Level

- Requires that the services will have an uptime (i.e., availability) of a certain percentage, during certain hours, measured over an agreed upon period.
- Example:

Provider will make the Services Available continuously, as measured over the course of each calendar month period, an average of 99.99% 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 Client. 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) Client's acts or omissions; (ii) Client's Internet connectivity; and (iii) Provider's regularly scheduled downtime (which shall occur weekly, Sundays, from 2 am – 4 am central time).

- Negotiate service level targets that address the client's business needs
- Downtime
  - Clients should receive written documentation of a provider's scheduled downtime and ensure the window creates no issues for the client's business
  - The provider should be pro-active in detecting downtime (e.g., require the provider to constantly monitor the "heartbeat" of all its servers through automated "pinging")
- Measurement Window
  - Providers tend to want longer measurement periods (e.g., quarterly) because they dilute the effects of a downtime and thus make remedies less available to the client

Service Levels – Service Response Time Service Level

- This service level sets forth maximum latencies and response times that a client should encounter when using the Services
  - Services that fail to provide timely responses to its users are effectively "unavailable"
- Specific service level target depends on the facts and circumstances in each case
  - Ex.
    - complexity of the transaction at issue
    - processing required
- Example:

Provider guarantees that __% of Service transactions will exhibit __ seconds or less response time, defined as the interval from the time the user sends a transaction to the time a visual confirmation of transaction completion is received.

Service Levels – Problem Response Time and Resolution Time Service Levels

- Providers often include only a response time measurement, which typically falls short of what is necessary
  - Response Time
    - measures the time period from when the problem is reported to when the provider notifies the client and begins working to address the issue
- Also, include a resolution time measurement
  - Resolution Time
    - measures the time period from when the problem is reported to when the provider implements a fix or acceptable workaround

Service Levels – Data Return Service Level

- The client should also consider adding a data return service level, if services involve
  - a critical business function, or
  - sensitive client information
- Measures the time period between the client's request for data and the provider's return of such data in accordance with the timeframe requirements of the agreement
- Provides additional assurance that client will be able to receive its data and continue to operate in the event that the provider stops providing services

Service Levels – Remedies

- Credits
  - Typically, remedies for failure to hit a service level start out as credits towards the next period's service
- Right to Terminate
  - If repeated failure occurs, the client should have the right to terminate the agreement without penalty or having to wait for the current term to expire
- 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, Client 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, Client 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 (a) three (3) months consecutively or (b) any three (3) months during a consecutive six (6) month period, then, in addition to all other remedies available to Client, Client shall be entitled to terminate this Agreement upon written notice to Provider with no further liability, expense, or obligation to Provider.

Data

- Client data issues
  - Security
  - Redundancy (i.e., Data Backups)
  - Ownership of Client Data
  - Use of Client Data
  - Data Conversion

Data – Security

- Why is data security important?
  - Provider may have possession of a client's most sensitive data, including data that may be subject to state and federal protections (e.g., personally identifiable financial and healthcare information)
  - Loss of such data or unauthorized disclosure of such data is a significant concern
    - Client may be unable to continue, or may be limited in, operating its business
    - Also, Client is ultimately accountable for complying with state and federal protections, regardless of where the data is stored

Data – Security

- Include specific contractual protections relating to information security, including specific details regarding
  - baseline security measures
  - security incident management
  - hardware, software and security policies
- Due Diligence
  - Conduct due diligence regarding the security practices of a provider
- Audit
  - Consider verifying the provider's capabilities via a physical visit or SAS 70 audit (IT internal controls audit) conducted by a third party, or both

Data – Security

- Provider's Security Policies
  - Compare the provider's policies to client's own
  - Confirm the provider's policies address security risks particular to cloud computing, and services being delivered over the Internet and accessible through a Web browser
    - Ex. #1: websites that use Adobe Flash and permit users to upload content, can be used by hackers to upload malicious Flash objects and launch attacks on users
    - Ex. #2: technologies used to facilitate scalability in a cloud computing solution, such as virtualization and multi-tenancy, may result in client data being stored on a physical server that also stores data of provider's other clients, which may increase the risk of unauthorized disclosure

Data – Security (example)

(a) In General. Provider will maintain and enforce safety and physical security procedures with respect to its access and maintenance of Client Information that are (1) at least equal to industry standards for such types of locations, (2) in accordance with reasonable Client security requirements, and (3) which provide reasonably appropriate technical and organizational safeguards against accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access of Client Information and all other data owned by Client and accessible by Provider under this Agreement.

(b) Storage of Client Information. All Client 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 for detailed information on Provider's security policies protections

(c) Security Audits. During the Term, Client 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 Client Information. Any of Client'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 within reasonable timeframes.

Data – Redundancy

- Include provisions regarding
  - the provider's duty to back up client data and the frequency of that back up, and
  - the client's access to such data or the delivery of such data to the client on a regular basis
- Compare the provider's backup policies to its own and make sure they are at least as stringent
- Example:

Provider will: (a) execute (i) nightly database backups to a backup server, (ii) incremental database transaction log file backups every 30 minutes to a backup server, (iii) weekly backups of all hosted Client Information and the default path to a backup server, and (iv) nightly incremental backups of the default path to a backup server; (b) replicate Client's database and default path to an off-site location (i.e., other than the primary data center); and (c) save the last 14 nightly database backups on a secure transfer server (i.e., at any given time, the last 14 nightly database backups will be on the secure transfer server) from which Client may retrieve the database backups at any time.

Data – Ownership and Use Rights

- Ownership
  - As previously mentioned, clarify that client has ownership of any data stored by the provider for client
    - In the event that the provider stops providing services and client is requesting the return of its data, there should be no separate dispute as to ownership of the data
- Use Rights
  - Confidentiality
    - Include specific language regarding the provider's obligations to maintain the confidentiality of client information
  - Use Limitations
    - Place appropriate limitations on the provider's use of client information (i.e., provider has no right to use such information except in connection with its performance under the cloud computing agreement)

Data – Ownership and Use Rights

- Provider's Proposed Use of Client Data
  - More cloud computing providers want to analyze and use the client data that resides on their servers for their own commercial benefit
    - Ex. provider may wish to use (de-identified) client data, aggregated along with other clients' data, to provide data analysis to industry groups or marketers
- Client should ask the provider about its uses and add a provider representation about which uses, if any, are permitted
- Most clients should conclude that the provider should not have any right to use the client's data, beyond what is strictly necessary to provide the services (whether in raw form, aggregated, or de-identified)

Data – Conversion

- Data conversion must be addressed to
  - avoid hidden costs, and
  - avoid being “locked in” to the provider’s solution
- Prior to Execution of Agreement
  - Confirm that
    - client data can be directly imported into provider’s services, or
    - any data conversion needed will be done at provider’s cost or at client’s cost (with client’s agreement)
  - Consider conducting a test run of provider’s mapping scheme
  - When checking provider’s references, ask about data migration experiences
- Expiration or Termination of the Agreement
  - Include explicit obligations on the part of the provider to
    - return the client’s data, both in provider’s data format and in a platform-agnostic format, and
    - destroy all of the client’s information on provider’s servers

Insurance

- Client should carry Cyber-Liability Insurance
  - Insure against IT risks, such as the following:
    - unauthorized access to a computer system
  - theft or destruction of data
    - hacker attacks
    - denial of service attacks
    - malicious code
    - security breaches of personal information
    - violations of state and federal privacy regulations
- Provider should be required to carry Errors and Omissions Liability Insurance and Commercial Blanket Bond, including Electronic & Computer Crime or Unauthorized Computer Access Insurance
  - Cover damages the client or others may suffer as a result of the provider's professional negligence and intentional acts by others (provider's employees, hackers, etc.)
  - Commercial General Liability Policy
    - It is critical that the client require the provider have more than just a commercial general liability policy (which may contain a professional services exclusion that precludes coverage for liability arising from IT services)

Indemnification

- The provider should agree to defend, indemnify, and hold harmless the client and its affiliates and agents from any claim
  - where the provider breaches its obligations in regards to the confidentiality and security of the client's data
  - that the services infringe the intellectual property rights of any third party
- Confidentiality and Security of Client's Data
  - intentional data breach
    - client should be fully indemnified
  - unintentional data breach
    - the provider may require a cap on its potential liability exposure
    - may be reasonable depending on the type of client data in question
- Third Party Intellectual Property Rights
  - provider may try to limit indemnification to
    - only infringement of copyrights
    - only patents "issued as of the Effective Date" of the agreement
    - only "United States" intellectual property rights
  - limitations are unacceptable – indemnification should extend to infringement claims of any "patent, copyright, trade secret, or other proprietary rights of a third party"

Limitation of Liability

- A fair limitation of liability clause must balance
  - the provider's concern about unlimited damages

  with
  - the client's right to have reasonable recourse in the event of a data breach or other incident

- A provider's limitation of liability clause usually provides:
  - Direct Damages Liability Cap
    - limits any liability of provider to the amount of fees paid under the agreement or a portion of the agreement (e.g., fees paid for the portion of the services at issue)
  - Indirect Damages Exclusion
    - excludes incidental, consequential (for example, lost revenues), exemplary, punitive, and other indirect damages

Limitation of Liability

- While a client may not be able to eliminate the limitation of liability in its entirety, the client should ask for the following:
  - Mutuality
    - The limitations of liability should apply to both parties
  - Exclusions
    - The following should be excluded from all limitations of liability and damages:
      - breach of the confidentiality provision by either party
      - claims for which provider is insured
      - the parties' respective third party indemnity obligations
      - either party's infringement of the other party's intellectual property rights
      - breach of the advertising/publicity provision
  - Direct Damages Liability Cap
    - Should be increased to some multiple of all fees paid (e.g., 2 to 4 times the total fees or the fees paid in the 12 months prior to the claim arising)
    - Note: The overall liability cap should not apply to the exclusions above.

Definition of Services

- The definition of “Services” in a cloud computing agreement should be broadly worded to allow the client full use of the services.
- Example:

“Services” shall mean Provider’s provision of software and infrastructure services described in Exhibit A (Services), and any other products, deliverables, and services to be provided by Provider to Client (i) described in a Statement of Work, (ii) identified in this Agreement, or (iii) otherwise necessary to comply with this Agreement, whether or not specifically set forth in (i) or (ii).

- Customizations
  - Identify up front any additional customizations needed
  - Typically a cloud computing offering may have more limited customization options, so that the provider can more efficiently manage the services and provide a more scalable solution

Fees

- Typically, a cloud computing service will be offered on a utility basis (i.e., “pay-as-you-go” or “pay-per-use” cost structure)
- The best time for the client to negotiate rates for incremental and decremental use is prior to signing the agreement.
- Clients should also attempt to lock in any recurring fees for a period of time (1-3 years) and thereafter an escalator based on CPI or other third party index should apply.

Termination

- Termination for Convenience
  - Client should be able to terminate the agreement at any time without penalty upon reasonable notice (14 to 30 days)
  - Minimum Commitment Period
    - Provider may request a minimum commitment period to recoup the provider's "investment" in securing the client as a customer (i.e., sales expenses and related costs)
    - If the client agrees, the committed term should be no more than 1 year and the provider should provide evidence of its up-front costs to justify such a requirement

Warranties

- Provider should warrant the following:
  - The services will perform in accordance with the specifications and, to the extent not inconsistent, provider's documentation
  - All services will be provided in a timely, workmanlike manner, in compliance with industry best practices
  - The provider will provide adequate training, as needed, to client on the use of the services
  - The services will comply with all federal, state, and local laws, rules, and regulations
  - The client's data and information will not be shared with or disclosed in any manner to any third party by provider without first obtaining the express written consent of client
  - The services will not infringe the intellectual property rights of any third person
  - The services will be free from viruses and other destructive programs
  - There is no pending or threatened litigation involving provider that may impair or interfere with the client's right to use the services
  - The provider has sufficient authority to enter into the agreement and grant the rights provided in the agreement to the client

Notification of Security Issues

- Include requirement that if
  - a breach of security or confidentiality occurs, and
  - it requires notification to client's customers or employees under any privacy law,
  - then client should have sole control over the timing, content, and method of such notification.

- Also, if the provider is culpable for the breach, then the provider should be required to reimburse client for its reasonable out-of-pocket costs in providing the notification

Pre-Agreement Provider Due Diligence

- Consider performing pre-agreement due diligence on the provider using a provider questionnaire
- Enables the client to
  - obtain a good idea of the extent to which the provider can meet the client's expectations, and
  - where gaps exist, eliminate them or negotiate through them.
- Examples of the items to cover in due diligence questionnaire:
  - provider's financial condition
  - insurance
  - existing service levels
  - capacity
  - physical and logical security
  - disaster recovery
  - business continuity
  - redundancy
  - ability to comply with applicable regulations

Conclusion

- Although there is no single widely accepted definition, cloud computing can be viewed as a service delivery model with the following features:
  - delivery over the Internet cloud,
  - both software and infrastructure resources provided as services,
  - scalability on-demand, and
  - payment based on the client's actual use and/or a period of time
- Benefits (i.e., cost reduction and service flexibility) should be weighed against risks to determine if cloud computing is appropriate for a company
- Similar to hosting and ASP agreements, the client needs to focus less on configuration, implementation, and acceptance and more on
  - service availability
  - performance (i.e., service levels)
  - security and control of the client's data

Contacts and Questions

Michael R. Overly, Esq. CISA, CISSP, CIPP, ISSMP, CRISC
Partner: Information Technology & Outsourcing
Foley & Lardner LLP
Tel: 213-972-4533
Fax: 213-486-0065