CLOUD COMPUTING – RISKS AND HOW TO MITIGATE THEM

Jeff Andrews

April 20, 2017

BRACEWELL

TODAY'S TOPICS

- Key Risks and Mitigating Contract Provisions
- Best Practices and Market Realities – Data Safeguarding, Data Breaches and Related Contract Provisions

KEY RISKS – WHAT MAKES THE CLOUD SPECIAL?

- Identical or near-identical services provided to multiple customers
- Services delivered from a remote location that may or may not be controlled by the vendor
- Vendor often utilizes shared resources to deliver services
- Services delivered over networks typically not controlled by the vendor

KEY RISKS – OVERVIEW

- Service Performance
- Unilateral Changes / Forced Changes
- Force Majeure
- Disaster Recovery
- Use of Customer Data
- Conversion & Return of Customer Data
- Audit Rights
- Changes to Fees
- Termination & Termination Assistance
- Limitations on Liability

KEY RISKS – SERVICE PERFORMANCE

- Risks:
  - Metrics do not measure what is important for a customer's operations
  - Process and exclusions make recovery of credits overly difficult
  - Credits are sole and exclusive remedy
- Solutions:
  - Ensure availability metric is set at least at 99.99%
  - Add metric for resolution/workaround for incidents/problems
  - Eliminate provisions requiring customer to report defaults for credit
  - Eliminate exceptions for matters within the vendor's control – eliminate blanket exception for matters outside of the vendor's control
  - Eliminate provision that credits are sole and exclusive remedy, or provide that credits are not the sole and exclusive remedy if performance is less than an agreed minimum amount
  - Add termination right for chronic failures

KEY RISKS – UNILATERAL CHANGES / FORCED CHANGES

- Risks:
  - Policies are incorporated by reference
  - Vendor reserves the right to make changes to, or even end-of-life, software
  - Vendor can force the customer to accept upgrades
- Solutions:
  - Changes cannot be adverse to customer (in customer's sole discretion, if possible)
  - Changes cannot require customer to incur additional costs or increase the fees owed the vendor
  - Reserve the right to terminate without payment of any termination fees

KEY RISKS – FORCE MAJEURE

- Risk: Any event beyond a party's "reasonable control"
  - Catch-all phrase at the end of the clause, preceded by the word "or"
  - Failures of subcontractors or suppliers?
  - Events that can be prevented or avoided (e.g., power failures and standby generators)?
  - Frustration of performance (e.g., economic events, governmental acts)?
- Solutions:
  - Limit weather events to extraordinary weather events
  - Exclude foreseeable weather events
  - Exclude strikes, lockouts and labor disputes of a party and its subcontractors and suppliers
  - Do not include the catch phrase "any event beyond a party's reasonable control"
  - To be excused, require a party to have used:
    - Reasonable precautions or commercially accepted processes to prevent the default or delay
    - Substitute services, alternate sources or work-around plans to circumvent the default or delay

KEY RISKS – DISASTER RECOVERY

- Risks:
  - Plan is incorporated by reference
  - Vendor reserves the right to make changes to the plan
  - Little to no detail (“trust us”)
- Solutions:
  - Ensure the plan is materially consistent with the customer’s policies
  - At a minimum, require RTOs and RPOs
  - Changes cannot be adverse to customer (in customer’s sole discretion, if possible), and cannot result in the plan being any less robust than as of contract signing
  - Reserve the right to terminate without payment of any termination fees

KEY RISKS – USE OF CUSTOMER DATA

- Risks:
  - Use of customer data as “necessary” to provide the services
  - Use of customer data for commercial purposes outside of the services
- Solutions:
  - Specify what uses of customer data are permitted / are not permitted
  - Prohibit use of data except in the performance of the contract
  - Specify that customer data is the customer’s confidential information
  - Require the vendor to represent and warrant that it will not otherwise use customer data
  - If ancillary use is truly necessary, require data to be used only in an aggregate form not capable of identifying customer or any individual

KEY RISKS – CONVERSION & RETURN OF CUSTOMER DATA

- Risks:
  - Data is converted into a format unusable by customer or successor vendors
  - Holding customer data hostage
- Solutions:
  - Specify the format in which customer data must be returned, or at least specify that customer data must be returned in an industry-standard, platform-agnostic format
  - Require return of all or any portion of customer data at customer's request and in accordance with customer's timeframe and instructions
  - Include express provision that the vendor shall not withhold any of the customer's data as a means of resolving any dispute

KEY RISKS – AUDIT RIGHTS

- Risks:
  - Lengthy and obtrusive
  - Potential claim / lawsuit in addition to payment of additional fees for excess usage
- Solutions:
  - No more than once per year upon set number of days' prior notice
  - Must be performed during customer's regular business hours; must not interfere with customer's business operations; must be completed within a set number of consecutive days
  - Make available records, but limit system access
  - Required customer assistance should not require customer to incur additional costs or require more than an agreed level of effort on the part of the customer's personnel
  - Specify a remediation process for excess use
    - Opportunity to purge / cease use
    - Payment of fees owed pursuant to the contract for use that is not purged / ended
    - Customer not responsible for fees for excess use authorized / permitted by vendor
  - Vendor's sole and exclusive recourse and remedy

KEY RISKS – CHANGES TO FEES

- Risks:
  - Vendor reserves the right to increase fees at any time, or periodically, without limits
  - Fee increases when vendor is acquired
- Solutions:
  - Specify that there are no fee increases during an initial term – use termination for convenience as negotiating position
  - Allow for set number of extensions, at customer's discretion and not automatic, with permitted fee increases once at the beginning of each extension period that are tied to CPI / ECI or capped at 3-5% and that are notified to customer at least a set number of days prior to expiration of then-current term
  - Pre-negotiate fee increases for renewals
  - Specify in assignment provisions that assignee is bound by all of the terms of the contract
  - Reserve the right to terminate without payment of any termination fees

KEY RISKS – TERMINATION & TERMINATION ASSISTANCE

- Risks:
  - Termination by the customer only permitted for the vendor's uncured material breach
  - Vendor is not contractually obligated to provide any termination assistance
- Solutions:
  - Ask for termination for convenience – offer to pay agreed termination fee
  - Add express termination rights for the following:
    - Specified breaches, such as chronic service level failures, disaster recovery failures and data breaches
    - Protracted force majeure events
    - Vendor's change in control and bankruptcy
  - Add provisions requiring the vendor to provide termination assistance
    - Include an attachment or provisions defining what assistance the vendor will provide, but at least require the vendor to provide all reasonable assistance requested by the customer in order to facilitate the transfer of the services
    - Agree in advance on the fees for termination assistance where the vendor must use resources that are not already included in the fees being paid by the customer
    - Agree in advance that the transition must occur in accordance with the customer's timetable, which will not require the vendor to complete the transition in less than an agreed period of time

KEY RISKS – LIMITATIONS ON LIABILITY

- Risks:
  - Liability limitations favor vendor (one-sided; small damages cap; no consequential damages)
  - Liability limitations cover all actions / claims and do not include typical exceptions
- Solutions:
  - Make limitations on liability mutual
  - Damages cap should be equal to 12 – 24 months of fees
  - Add typical exceptions for:
    - Indemnification claims and obligations
    - Breaches of confidentiality obligations
    - Gross negligence, willful misconduct and fraud
  - Include a separate damages cap for data breaches (establish at $221 per record)
  - Add provisions designating certain damages as agreed direct damages
    - Costs of cover
    - Costs incurred in connection with data loss and breaches (*e.g.*, notice, investigation, remediation, etc.)

DATA SAFEGUARDING – BEST PRACTICES

In an ideal world…

"Vendor will establish, institute, monitor, maintain and comply with a written system and information security program (the "Data Safeguards") that includes administrative, technical and physical protocols and controls to safeguard physical and electronic access to Customer Data, and to prevent, detect, respond to and recover from any unauthorized disclosure, access, destruction, loss, damage, alteration or use of Customer Data, that in each case is in Vendor's possession or control. The Data Safeguards will comply with Customer's then-current data security requirements and policies and will be no less rigorous than the most stringent of (a) Vendor's then-current data security requirements for data of a similar nature, (b) industry standards specified in this Agreement, including ISO 27001:2013 (Information technology – Security techniques – Information security management systems – Requirements) and ISO 27002:2013 (Information technology – Security techniques – Code of practice for information security management), and (c) any systems or data security requirements specified elsewhere in this Agreement or required by applicable law. Vendor will review and test (and re-test as necessary) at least annually the Data Safeguards to assess adherence to and the effectiveness of the Data Safeguards, and implement action plans to remediate identified vulnerabilities and deficiencies."

DATA BREACHES – BEST PRACTICES

In an ideal world…

"Upon any loss or theft, or unauthorized access, disclosure, copying, use or modification of, any Personal Data that is in Vendor's possession or control, only Customer, in its sole discretion, may determine whether and when notice of any such event will be provided to any affected persons or governmental authorities or similar third parties, including pursuant to applicable laws. Customer will have final editorial control over the content of any filings, communications, notices, press releases or reports related to any such event. Vendor will reimburse Customer for all costs and expenses incurred by Customer in connection with investigating, addressing and responding to any such event, including (a) forensic and investigation services to investigate the existence and cause of the event and the extent to which Personal Data was involved, (b) preparation and mailing or other transmission of notifications or other communications to any affected persons or governmental authorities or similar third parties as Customer deems appropriate, (c) establishment of a call center or other communications procedures in response to the event, (d) credit monitoring, identity theft monitoring, fraud resolution and repair services for the affected persons, (e) public relations and other similar crisis management services, (f) legal, consulting and accounting expenses associated with Customer's investigation of and response to the event, and (g) any governmental fines or penalties."

DATA BREACHES – BEST PRACTICES

In an ideal world…

"If Vendor discovers or is notified of a suspected or actual loss or theft, or a suspected or actual unauthorized access, disclosure, copying, use or modification, of any Customer Data in its possession or control, then in each case Vendor will:

(a) within twenty-four (24) hours of becoming aware thereof, notify Customer of the date and circumstances of such event, the nature and content of the Customer Data so affected (including, if the event involves any Personal Data, the number of persons affected and, to the extent possible, the identities of the affected persons), and the steps Vendor has taken to investigate the event, mitigate potential harm and prevent further loss or theft, or further unauthorized access, disclosure, copying, use or modification of, the Customer Data so affected;

(b) assemble and preserve pertinent information with respect to the event;

(c) conduct a root-cause analysis to determine the cause(s) of the event, and provide Customer with a detailed report indicating the cause(s) of the event and the plan to address the event;

(d) document actions taken in response to the event in sufficient detail to meet reasonable expectations of forensic admissibility, and conduct a post-incident review of all events and actions taken, if any, with a view to making any needed modifications relating to the protection of Customer Data..."

DATA BREACHES – BEST PRACTICES

continued from previous slide…

"(e) as requested by Customer, advise Customer of the status of remedial efforts being undertaken with respect to the event;

(f) cooperate with any investigation relating to the event that is carried out at the direction of any governmental authority;

(g) cooperate with Customer in all reasonable and lawful efforts to investigate, prevent the recurrence of, mitigate and rectify the event;

(h) minimize the impact of and correct any problems that contributed to the event; and

(i) take appropriate preventive measures so that such problems do not recur, including implementing new security measures to the extent reasonably requested by Customer."

Back-up the obligations set forth on slides 16, 17 and 18 with indemnities and exclusions from the limitations on liability!

DATA SAFEGUARDING – MARKET REALITY

- Vendors will not agree to comply with unique customer requirements, except with private cloud arrangements
- Vendors will not agree to keep their data safeguards consistent with market standards
- Some vendors will limit distribution and examination of their security policies
- Some vendors will even not agree that a customer's data constitutes the customer's confidential information

DATA SAFEGUARDING – MARKET REALITY

So what do you do?

- Ensure that SMEs review and accept the vendor's security and privacy policies prior to contract signature, and conduct site visits if possible
- Make certain the contract includes a provision requiring the vendor to comply with applicable law
- Incorporate the vendor's security and privacy policies by reference into the contract
- Changes to the vendor's policies cannot be adverse to customer (in customer's sole discretion, if possible), and cannot result in them being any less robust than as of contract signing
- Reserve the right to terminate without payment of any termination fees

DATA BREACHES – MARKET REALITY

- Vendors resist obligations that require burdensome steps across their entire customer base
- Many vendors seek to retain the right to provide their own breach notices, and approve a customer's breach notices
- Most vendors will not agree to reimburse their customers for costs incurred in connection with a data breach
- Most vendors will not agree to assume unlimited liability for data breaches
- Some vendors even hold their customers responsible for costs of breach notices to the customer's employees and its customers

DATA BREACHES – MARKET REALITY

So what do you do?

- Include a separate damages cap, ***or*** if that is not acceptable an enhanced damages cap, solely covering losses resulting from data breaches
- Allow for the recovery of consequential and indirect damages within the separate damages cap, ***or*** if that is not acceptable have the vendor contractually acknowledge that costs incurred in connection with a data breach are direct damages
- Request an indemnity from third party claims resulting from the breach; push to have the indemnity excluded from the limitations on liability
- Retain sole control over the content, timing and method of notices
- Do not permit the vendor to notify affected persons
- Reserve the right to terminate without payment of any termination fees

QUESTIONS?

JEFF ANDREWS, PARTNER

jeff.andrews@bracewell.com
T: +1.713.221.1439

This presentation is provided for informational purposes only and should not be considered specific legal advice on any subject matter. You should contact your attorney to obtain advice with respect to any particular issue or problem. The content of this presentation contains general information and may not reflect current legal developments, verdicts or settlements. Use of and access to this presentation does not create an attorney-client relationship between you and Bracewell.

BRACEWELL