When The Cloud Goes Bust: Data Breaches In The Cloud

CHRISTOPHER PIERSON, PH.D., J.D.
LSQ

JAMES T. SHREVE, ESQ.
BUCKLEYSANDLER LLP

Session ID: CLD-107
Session Classification: Intermediate

RSA CONFERENCE 2012

Scenario 1 - Paris . . .

- FBI identifies PII on a French drop site
  - Data reviewed and IP's traced
  - Exfiltration 1 year ago
  - CloudCo is notified
- CloudCo is your IaaS provider
  - PII of your customers
  - Notifies you of discovery
  - No further details
- Now What?

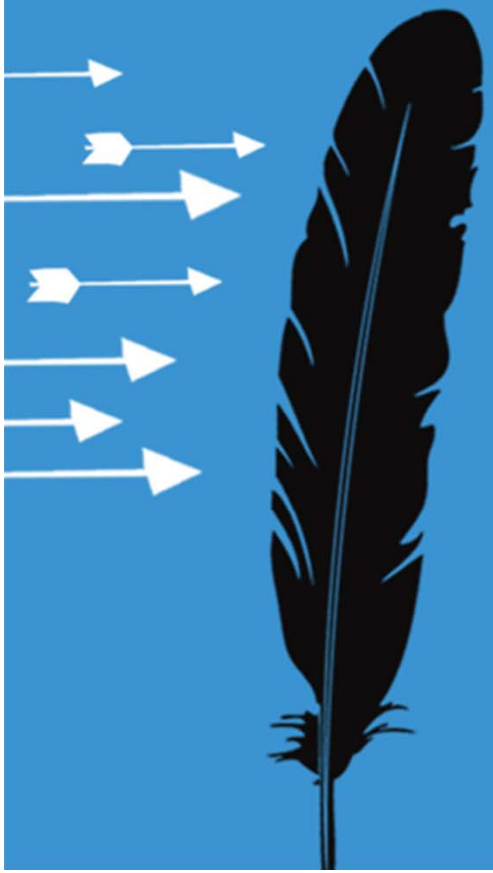
Scenario 2 – Improper Permissions

- Data stored with cloud provider on hybrid cloud
- Notice from provider
  - Permissions improperly set for some users
  - At least some employees of other companies could view company materials
  - Uncertain of extent or timeframe

Be prepared - grab an umbrella

Indemnification is after the fact . . .

The opinions contained herein do not reflect the opinions and beliefs of the author's employers. All content contained herein is for informational purposes only and may not reflect the most current legal developments. The content is <u>not offered</u> as legal or any other advice on any particular matter.



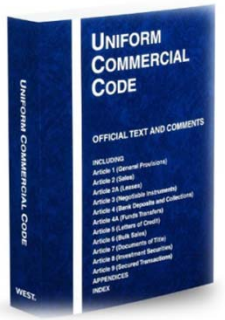
Three-Pronged Attack!

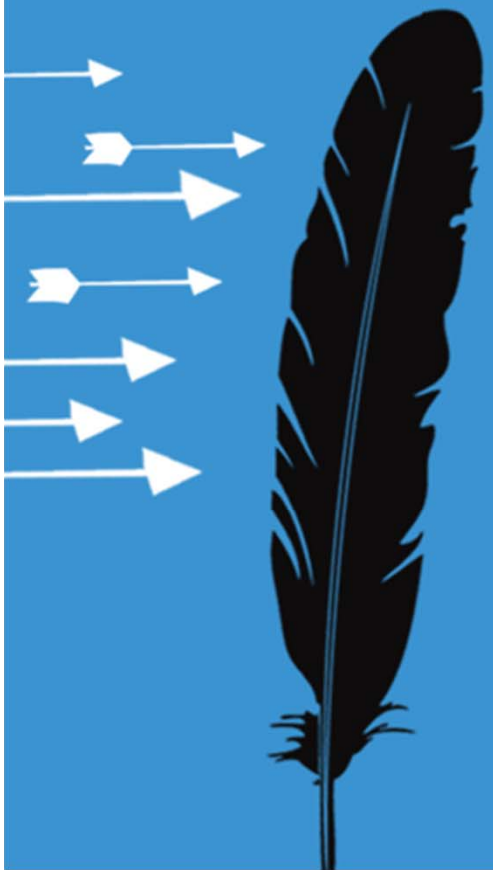
Three Prongs to Mitigate Loss Scenario

1. Playing Field: Contract
   - Major issues are clear
   - Address up front

2. Front End: Due Diligence
   - Test things out
   - InfoSec and Assurance

3. Back End: Regulatory & Legal

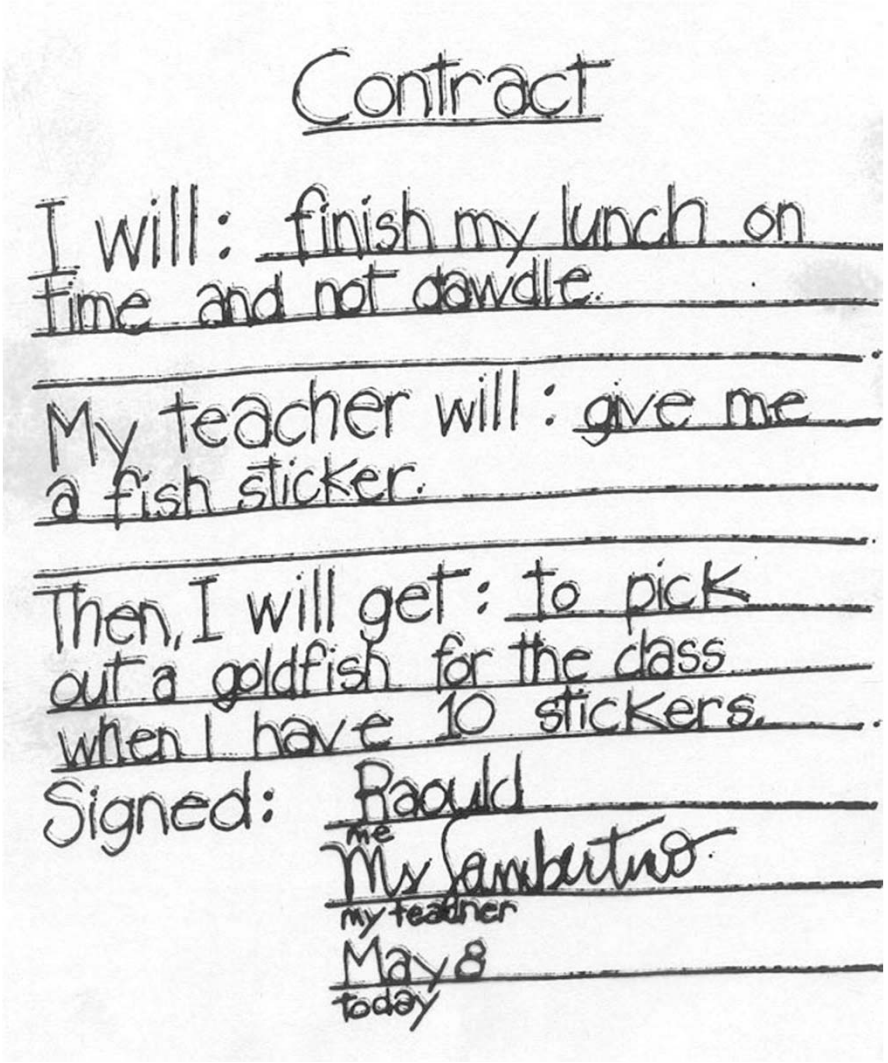




Contracts

Contracts – address the foreseen issues

- Cover the known risks (e.g., incidents with similar entities, authentication)
- Be in contact with legal before and during negotiations
- Leverage - Have plans B, C & D
  - Livable standards other than the preferred

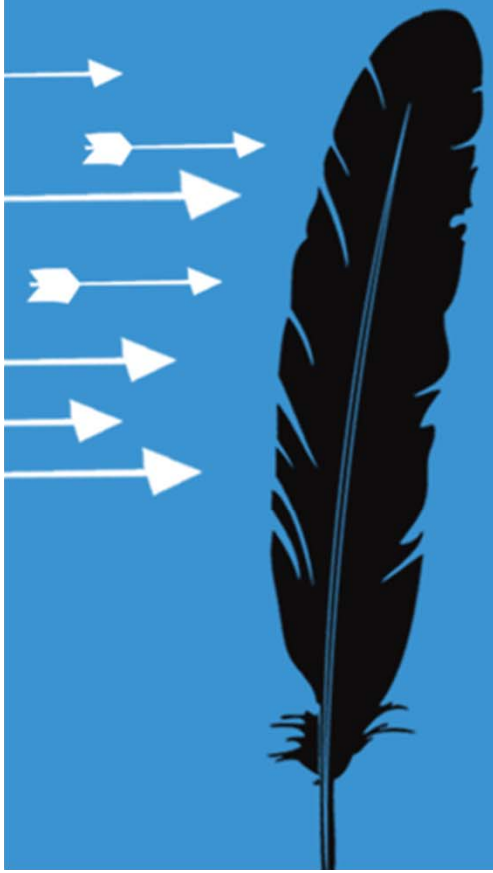


Contracts – areas to cover

- Indemnity
  - Calculate costs to the business of access loss, data corruption, etc. beforehand to the extent possible
  - Be as complete as possible (consequential damages)
- Actual and possible breaches
  - Make sure **you** determine what is a breach
- Access to external forensics and experts
  - Situations may call for outside persons to access the system, especially for a regulated entity
- Exiting the cloud
  - No liens or other means to hold data captive

Contracts - scenarios

- Information
  - What are they obligated to provide under the contract
- Responsibilities
  - What has the provider assumed
- Timing
  - When does the clock start
- Costs
  - How much of losses are covered



Cyber Due Diligence

Cyber Due Diligence - infosec

- Authentication/Access
  - Who am I?
    - Rise of Multi-Layered Authentication
    - Managed Authentication by the Vendor
  - What can I do?

- OPSEC
  - Security is geographic
  - Political, Cultural, Geographic Risks & Threats

- Downstream Risks
  - 2nd Party, 3rd Party
    - Subcontracting the load
    - Subcontracting globally
    - Role of US v. EU laws
  - Can you limit this?
    - Practical considerations
    - Regulating v. Restricting

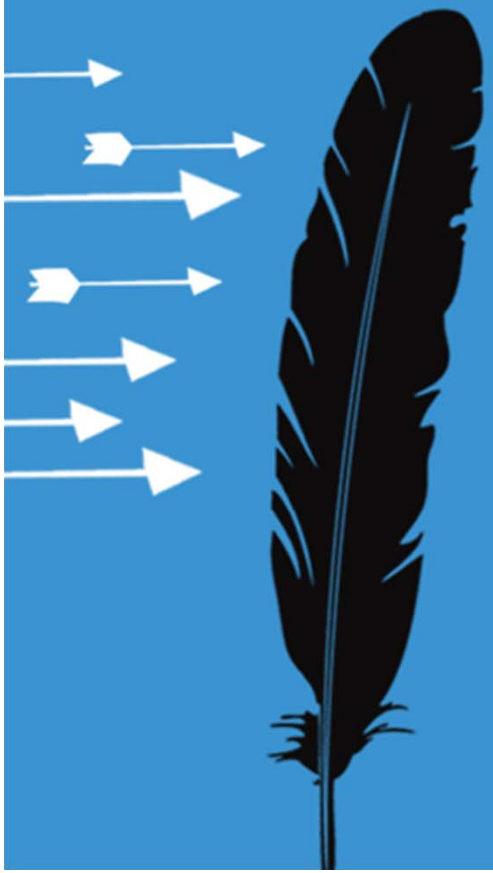
Cyber Due Diligence – audits/assurance

- Assurance or Assurances?
  - Self-Certifications & Their Role
    - SAS70 (Statement on Auditing Standards)
    - SSAE 16 (Statement on Standards for Attestation Engagements)
    - SOC2 and SOC3 (Service Organisation Control)
  - Increase of Third Party Assessments
    - BITS, Shared Vendor Assessment

- Is it security?
  - Reliance in Audits
  - Reliance in Court
  - Reliance for Insurers

Cyber Due Diligence – tenants & roaches

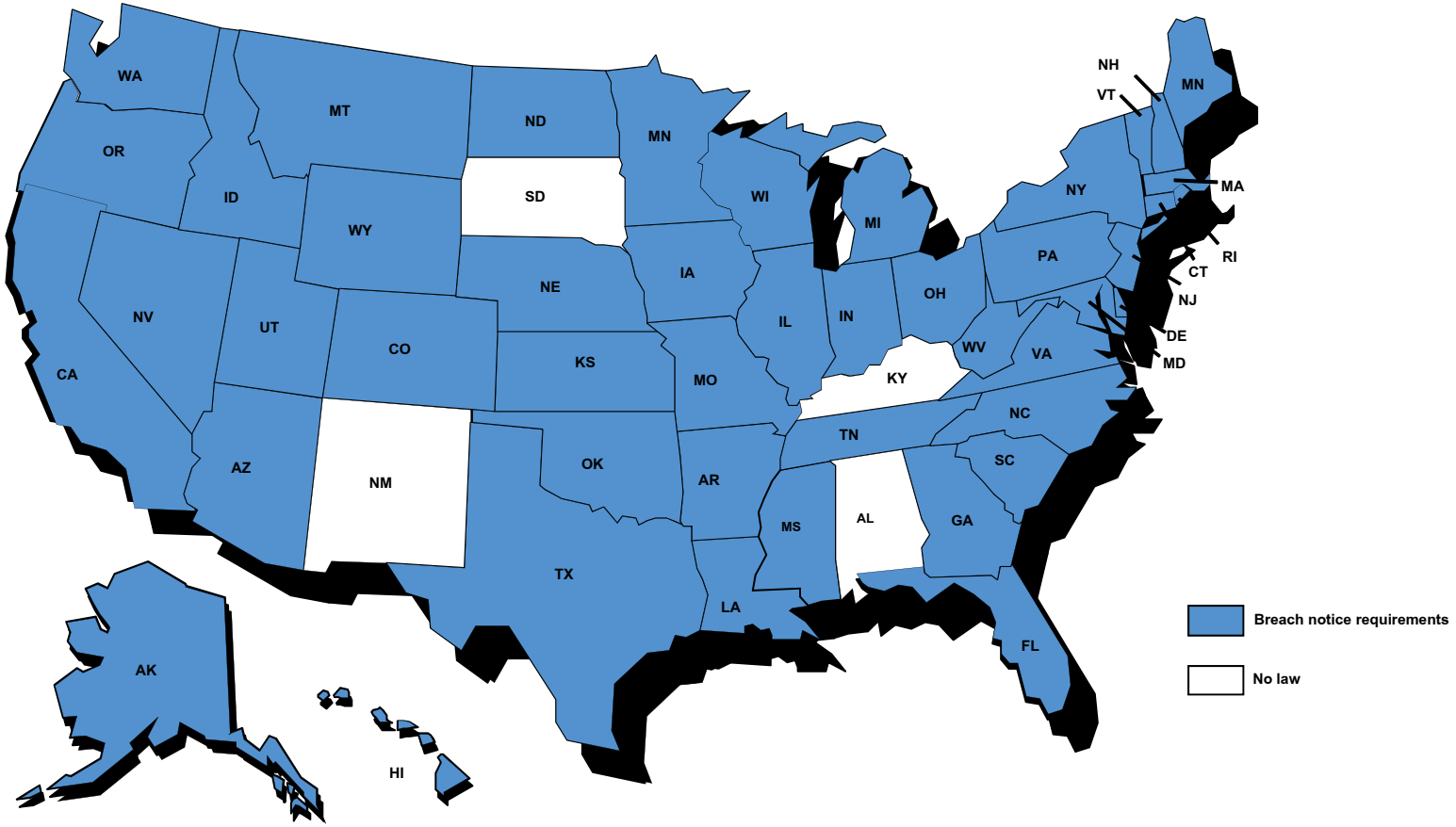
- Tenants
  - Single residency
  - Multi-tenancy
  - Penthouse – does it matter?
- Type of Service
  - Iaas v. SaaS
- Forensics
  - QSA for PCI-DSS Compliance
  - Multiple Providers
  - In-House Expertise
  - External Approved List
  - Federal LEO Investigations



Regulatory & Legal Waters

US Breach Notice Requirements

State Laws



Also, federal requirements for banks and health care and related entities.

Non-US Breach Notice Requirements

- Austria
- Australia
- Canada
- France
- Germany
- Hong Kong
- Ireland
- Japan
- Mexico
- United Kingdom
- Uruguay

More EU state requirements to come

Regulatory & Legal Waters

- Lots of Cloud Cover
- Clouds in US & in the EU, but different
- German Clouds

- Who is the meteorologist?
- How do these forecasts differ?
- Why do the models not track to one another?

Regulatory & Legal Waters

- Separate incident response program for cloud incidents
  - Time

Regulatory & Legal Waters

- FBI seizes servers from the cloud
- Collateral Damage?
- SLA's
- NSL's
- Resiliency Questions

FBI Seizes Public Cloud Servers Killing Innocent Applications

JULY 3, 2011 LEAVE A COMMENT

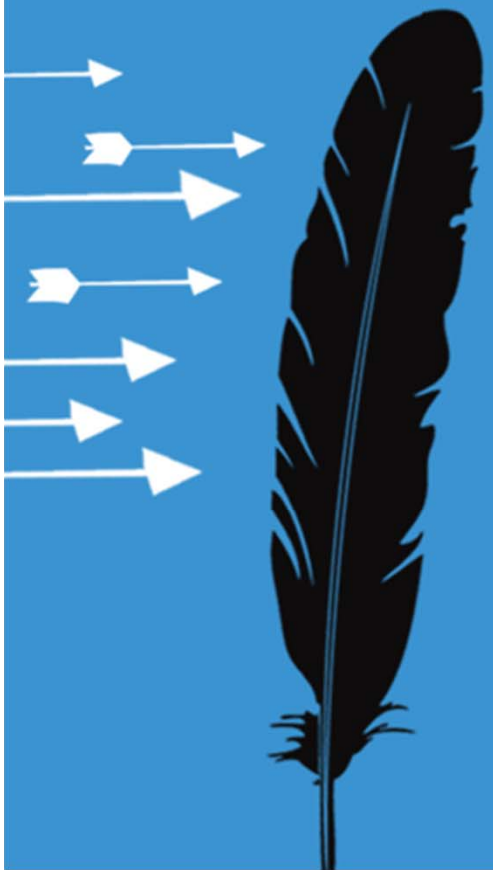
5 Votes

In my May 24 blog entry Amazon, Sony, Hackers and the Public Cloud, I described a potential risk to users of public cloud services:

"There's this little thing called the Patriot Act that allows the FBI and others to do just that – walk into Amazon's data center and remove the machine running the hackers applications – and mine along with them. And if I have a complex transactional application it's very likely that I will lose something."

Just a couple of weeks later, that risk became reality – though admittedly the incident did not occur at Amazon, but at a data center in Reston, Virginia used by Swiss hosting provider DigitalOne AG. At 1:15am, the FBI arrived, and seized 62 servers, ripping out their cables and removing them from three separate enclosures. The effect, accordingto DigitalOne was *"massive disruption to our business and functional processes to our clients' uninvolved servers"*.

DigitalOne claim that prior to the seizure, the authorities had requested information on three IP addresses. DigitalOne precisely identified the three servers using those IP addresses to the FBI agents, but the agents seized a further 59 servers that were present in the same enclosures. DigitalOne also claim that *"various modules and cable connections, and also our company's backup systems were affected, resulting in massive disruptions to a considerable number of client servers, our e-mail system, and our support system"*.



Where Do I Go From Here?

What Can I Do?

- Contracts:
  - Research several cloud providers
  - Review their standard contracts with counsel
  - Determine what is crucial versus nice to have
  - Have a negotiable middle ground
  - Plan ahead of time for highest risk threats
  - Table top these from a legal perspective
  - Highlight and respond to issues

What Can I Do?

- You can offshore/outsource the task, but you still own the risk
  - Information security due diligence
    - Robust, written programs, on-site investigations
  - Insurance
    - Cyber insurance a must, CGL does not cover
  - Other mitigants
    - Physical security
    - Pre-employment screening
  - Safety in numbers
    - Number of other co-located tenants
    - Similar infrastructure tenants
  - Communicate openly with regulators
  - Industry associations

What Can I Do?

- GOVERNANCE
  - From the top
    - Board of Directors has oversight/ownership
    - Committee discussions, progressions, structure
    - Executive involvement, not rubber stamping
    - Executive oversight and minuted discussions
  - Beyond committees
    - Instill culture of issues, discussions, root causes and ACTION
  - Best-in-Class
    - Benchmarking against institutions of similar size and complexity
    - Member associations (e.g. Financial-BITS)

Resources:

- Cloud Security Alliance - https://cloudsecurityalliance.org/
- CSA Security Document - https://cloudsecurityalliance.org/research/security-guidance/
- NIST - www.nist.gov/itl/cloud/

Thanks & Contact Information!

Christopher T. Pierson, Ph.D., J.D.
EVP, Chief Security Officer
& Chief Compliance Officer
LSQ
(Orlando, FL)
cpierson@lsq.com

James T. Shreve, Esq.
Attorney
BuckleySandler LLP
202.461.2994
(Washington, DC)
jshreve@buckleysandler.com