Take it or Leave IT: Pitfalls and Challenges of IT Contracts

Prepared by Deputy City Attorneys Margarita Gutierrez and Rosa M. Sánchez – Office of the San Francisco City Attorney

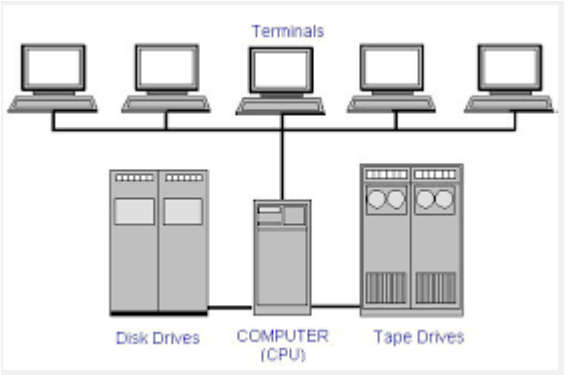
League of California Cities, Spring 2017 Conference
May 4, 2017

Software as a Service (SaaS)
How did we get here?

- SaaS is considered to be part of the nomenclature of cloud computing.
- SaaS is a software licensing and delivery model where the software is owned, hosted and licensed on a subscription basis by the contractor either at the contractor's or its subcontractor's data centers. Upgrades or updates, both major and minor, are rolled out continuously, and without customer review or approval.
- SaaS is usually sold on a subscription model, meaning that users pay a monthly fee rather than purchasing a license upfront.

History continued. . .

- Centralized hosting of business applications dates back to the 1960s (IBM and other mainframe providers conducted a service bureau business often referred to as time-sharing or utility computing).



History continued. . .

- The expansion of the internet during the 1990s brought about a new class of centralized computing, called Application Service Providers (ASP) (hosted specialized business applications with the goal of reducing costs)

History continued. . .

- SaaS essentially extends the idea of the ASP model.
- As of 2012, SaaS contractors typically develop and manage their own software.
- SaaS solutions rely predominantly on the Web and only require a web browser to use.
- SaaS solutions normally utilize a multitenant architecture, in which the application serves multiple businesses and users and partitions its data accordingly.

Software as a Service

- The National Institute of Standards and Technology (NIST) defines Cloud Computing as: “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and releases with minimal management effort or service provider interaction.” Three common service models include, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Is a hosted environment the appropriate information technology solution for a City department? Items to consider:

1. Sensitivity of data
2. On-line hosting facility security
3. Ownership and location of data
4. Disaster recovery and location of the primary and back up data centers
5. Availability of data
6. Termination provisions and vendor bankruptcy

Items to consider, continued…

7. Audits
8. Records Retention Policy and litigation holds
9. Public Records Requests and/or Subpoenas
10. Limitation on Click-Wrap Disclaimer
11. Disabling Code
12. Dispute Resolution/Venue

DATA BREACH CONSIDERATIONS

1. Data Breach
2. Remedies
3. Insurance
4. Recovering damages

DATA BREACH

Data Breach “unauthorized acquisition or “reasonable belief” of unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency.

Cal. Civ. Code §1798.29 (a) & (f). “California Information Privacy Act”

What are you protecting? What was breached?

Personally Identifiable Information "PII"

any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.
Cal. Civ. Code §1798.29 et seq.

Protected Health Information "PHI"

HIPAA & HITECH [42 CFR Parts 160-164]: protects PHI (2 CFR Part 2: protects information obtained by federally-assisted substance use programs

CMIA-Civil Code § 56 et. seq Confidentiality of Medical Information Act

Lanterman Petris Short Act (LPS) [Welfare & Institutions Code § 5000 et. seq.]Mental Health: Medical information kept by a licensed health facility: [Health & Safety Code § 1280.15]

HIV data: H & S Code § 120820 (used in investigations); § 120975-121020 (mandated blood tests for public health); § 121025 (state/local public health agencies); § 121065 (test results of source patient); Insurance Code § 799.03 (tests requested by insurers); Penal Code §§ 7530 & 1202.6 (inmates and convicted persons)Substance Use: [Health & Safety Code § 123125]

This list is not exhaustive – Financial Records, Criminal Justice Records, Employee Records

What can we do?

Work with the limitation of liability, if at all possible work in a carve-out for damages arising out of the vendor's willful or reckless misconduct so that the cap will apply only to simple negligence.

No limitation or exclusions will apply to liability arising out of either party's (1) confidentiality obligations (except for all liability related to Customer Data, which will remain subject to the limitations and exclusions above); (2) defense obligations; (3) violation of the other party's intellectual property rights; *or (4) liability for damages caused by either party's gross negligence or willful misconduct and awarded by a court of final adjudication (provided that, in jurisdictions that do not recognize a legal distinction between "gross negligence" and "negligence," "gross negligence" as used in this subsection shall mean "recklessness").*

P.F. CHANG'S CHINA BISTRO

- Policy marketed at " a flexible insurance solution designed to by cyber risk experts to address the full breadth of risks associated with doing business in today's technology dependent world that covers direct loss, legal liability, and consequential loss resulting from cyber security breaches."

- Breach happens. (Computer Hackers had obtained and posted online approximately 60,000 credit card numbers belonging to customers.)

- Insurer covers costs of forensic investigation and the costs of defending litigation filed by customers whose credit card information was stolen.

- Insurer refused to cover fees assessed by Bank of America Merchant Services (The Fraud Recovery Assessment, Operational Reimbursement Assessment and Case Management Fee).

P.F. CHANG'S CHINA BISTRO

Bank of America

In no less than three places in the MSA does Chang's agree to reimburse or compensate BAMS for any "fees," "fines," "penalties," or "assessments" imposed on BAMS by the Associations, or, in other words, indemnify BAMS. More specifically, Section 13.5 of the Addendum to the MSA reads: "[Chang's] agrees to pay [BAMS] any fines, fees, or penalties imposed on [BAMS] by any Associations, resulting from Chargebacks and any other fines, fees or penalties imposed by an Association with respect to acts or omissions of [Chang's]."

Cost/Benefit

Annual Insurance Premium

$134,052

Costs of forensic investigation litigation defense - Covered by Insurance

$1,700,000

Fees assessed by BAMS that Insurance refused to Cover

$1,929,921.57

RESOURCES

California Attorney General's List of State and Federal Privacy Laws
https://oag.ca.gov/privacy/privacy-laws

California Department of General Services

http://www.dgs.ca.gov/pd/Home/CloudComputing.aspx

NIST Publication

http://csrc.nist.gov/publications/PubsSPs.html#800-145

http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf

SSAE Security Guidance

http://ssae16.com/SSAE16_overview.html

Practising Law Institute - The Ethics of Electronic Information 2016, 17th Annual Institute on Privacy and Data Security Law, Cloud Computing 2016 – Key Issues and Practical Guidance