Data Security: Public Contracts and the Cloud

July 27, 2012
ABA Public Contract Law Section, State and Local Division

Ieuan Mahony | Holland & Knight
.ieuan.mahony@hklaw.com
Roadmap

• Why is security a concern?

• Why “outsource” security?

• Why the cloud?
  – (and what in the Sam Hill is “the cloud”?)

• What are the alternatives?
“Flavors” of Exposure

• External unfriendly threats = hackers and competitors

• External friendly threats = service providers

• Internal threats = employees and consultants

• Business model threats = no risk assessment; unprepared
Statistic

• April 2012 report from Massachusetts regulators:
  – Approximately 1,800 data breaches
  – Over the past four years.

• “High scoring” industries
  – Financial services: 955
  – Health care: 214
  – Education: 101
Brief Examples

• Sony
  – credit card data of PlayStation Network users
  – 77 million user accounts
    • name,
    • address (city, state, zip),
    • e-mail address, birthdate,
    • PlayStation Network/Qriocity password and login

• Health Net
  – Data servers missing for a month
  – 2 million customers nationwide
  – Social Security numbers and health history
Exposure to Regulators

• FTC enforcement powers under (e.g.):
  – Fair Credit Reporting Act (FCRA)
  – Gramm-Leach-Bliley Act (GLBA)
  – Children's Online Privacy Protection Act (COPPA)
  – More important: general jurisdiction over unfair or deceptive acts

Other Exposure

• Plaintiff Class Actions
  – In re iPhone Application Litigation, (N.D. Cal., Sept., 2011)
  – In re Facebook Privacy Litigation, (N.D. Cal., May, 2011).

• Claims by business partners

• Exposure to credit card issuers under PCI-DSS

• Public perception and damage to goodwill

• Particular concerns when dealing with public entities
• What is the value I see here?
• What am I going to do with it?
• How am I protecting it and how should I protect it?
Options

• Local hosting
• Engage data center
• Obtain managed services, e.g.
  – Provisioning
  – Remote backup
  – Secure archiving
  – Disaster recovery
• Move “to the cloud” fully
• Costs, risks, and benefits
All Computing Resources

- Application Software
  - “SaaS” – Software as a Service

- Operating System Platform
  - “PaaS” – Platform as a Service

- Infrastructure
  - “IaaS” – Infrastructure as a Service

Traditional Assets
Cloud Services
What are key characteristics of cloud computing?
• **Multi-tenanted**: computing resources are pooled and (often) shared by multiple subscribers
• **Virtual resources**: logical (virtual) resources are dynamically assigned based on demand
• **Location independent**: subscriber assets may be disbursed over many physical locations
• **On-demand self-service**: subscriber needs are (at least theoretically) provisioned automatically and as required
• **Broad network access**: access available through browsers
• **Elasticity**: scale up and down
Cloud Deployments

- **Private cloud**: for a single organization
- **Community cloud**: for several organizations, with shared cloud infrastructure and shared concerns
- **Public cloud**: for the general public
- **Hybrid cloud**: a combination of two or more clouds
Legal Implications

• Players
  – Cloud Service Provider (“CSP”)
  – Independent Software Vendors (“ISVs”)
  – Telcos
  – Subscribers to CSP’s services
  – Individual end users
  – CSP’s Competitors

• Regulatory Compliance and Risk Areas
  – Privacy [COPPA, HIPAA, GLBA, DPA]
  – Security
  – Intellectual property issues
  – Open Source / interoperability / standards
  – Tort exposure
  – Responsibility for users’ conduct
  – Document Retention and electronic discovery
  – Terrorism, surveillance, preservation
  – Taxation
  – International, export & cross-border
  – Personal jurisdiction

• Tools to Manage Risk
  – Contracts
  – Service Level Agreements (“SLAs”)
  – Clear service boundaries
  – DMCA, CDA, ECPA
  – Pricing
  – Insurance
  – Lobbying

• Assets
  – Products / IPR
  – Ecosystem
  – Data: yours / others’
  – Uncoupling assets: portability
Security

• Data is vulnerable during:
  – Transmission
  – Cloud storage

• Security measures include:
  – Firewall protection
  – User authentication
  – Access controls
  – Data segregation
  – Encryption
Independent Assessment

• Statement for Attestation Engagements No. 16 (“SSAE 16”),

• Statement on Auditing Standards No. 70: Service Organizations (“SAS 70”)

• From the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA)

• These defines the professional standards used by a service auditor to assess the internal security and other controls of a service
Security Standards

• The standards for compliance are generally “relative”
• Weighing the costs of added security against the risks and results of security compromise
• To achieve this “balance” legal and technical resources must communicate
• A common previous approach:
  – We will use “reasonable efforts to secure your data”
Sample Standards

• Federal Trade Commission Act (15 USC §§41-58, as amended);
• Electronic Fund Transfer Act (15 USC §1693 et seq.);
• Federal Reserve Regulation E (12 CFR Part 205);
• Identify Theft and Assumption Deterrence Act (18 USC §1028);
• Fair Credit Reporting Act (15 USC §1681 et seq.);
• “Red Flag” Rule (16 CFR Part 681 and analogous regulations, as applicable);
• Gramm-Leach-Bliley Act (15 USC §§6801-6809 and §§6821-6827);
• Financial Privacy Rule (16 CFR Part 313 and analogous regulations, as applicable);
• The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") (including regulations and rules under HIPAA and the HITECH Act);
• Safeguards Rule (16 CFR Part 314 and analogous regulations, as applicable);
• USA PATRIOT Act (115 Stat. 272);
• Federal Regulation II (12 CFR Part 235);
• Notice of Security Breach Regulations; and
• Information Security Regulations.
Central Role Of Risk Assessment and Resulting Policies and Practices

• Risk assessment
  – Sets the internal “relative” standard tailored to your entity
  – Good process = business justification for selected level of security

• Written information security policy
  – Physical site security
  – Network security
  – Encryption

• PCI-DSS validation
  – QSA – qualified security assessor (outside
  validation of compliance with PCI-DSS requirements)
Service Providers - The “Stack”

• You are responsible to safeguard service providers’ activities

• Keep in mind, as well, the “chain” of entities that might “touch” the data

• Complex stack, for example in mobile networks and the mobile app ecosystem
  – the handset maker,
  – the carrier,
  – the platform provider,
  – the third-party analytics company,
Challenges...
22. SECURITY
   22.1. Required Physical Security Measures
   22.2. Required Technical Security Measures
      22.2.1. User Authentication
      22.2.2. Access Controls
      22.2.3. Encryption
      22.2.4. Firewalls; Virus Protections
   22.3. Information Security Policies and Practices
      22.3.1. Risk Assessments
      22.3.2. Monitoring and Continuous Improvement
      22.3.3. Employee Practices
   22.4. Subcontractor Security Obligations
   22.5. Third Party Security Obligations
   22.6. Contractor Responsibility for Subcontractor and Third Party
         Compliance with Security Obligations
   22.7. Disaster Recovery and Business Continuity
   22.8. Incident Response Plan; Incident Response
      22.8.1. Notice of Intrusion; Implementation of Plan
      22.8.2. Contain Exposure
   22.9. Privacy and Security Regulations
   22.10. SSAE 16 Audit
      22.10.1. Timing
      22.10.2. Provision of Report to Authority
      22.10.3. Contractor Inability to Deliver
   22.11. Additional Requirements Concerning Sensitive Security
           Information
   22.12. Contractor Designation As Data Controller or Data Processor
23. Payment Card Security Standard
   23.1. Compliance with Standard
   23.2. PCI-DSS Vendors
   23.3. Validation
   23.4. Reports And Confirmations To The Authority
   23.5. Authority-Requested Validation
      23.5.1. Process
      23.5.2. No Effect On Contractor Obligations
      23.5.3. Costs of Authority-Requested Validation
   23.6. Remediation
   23.7. Notice to Payment Card Networks
   23.8. Responsibility for Penalties
   23.9. Relationship to Other Data Security Provisions
Conclusion

- New developments
- New challenges
- Proactive *not* reactive