Scrambling for Compliance

Reworking Your Information Technology Service Contracts

Security Camp
Boston University
Boston, MA
August 20, 2009
[REVISED TO REFLECT PROPOSED REVISIONS TO MASSACHUSETTS REGULATIONS ANNOUNCED August 17, 2009]]

John J. Smith, VistaLaw International, LLC

Overview of Presentation

- Why “scrambling” ? [Massachusetts deadline moved out to March 1, 2010]
- Why “reworking”? [selecting and retaining vendors]
- Key Elements of Information (Data) Security Regulations
- Massachusetts “Standards”: the Template for Compliance Programs?
- Our focus today --

  IT vendor relationships, contract management practices
  - Self-auditing; reopening settled contracts
  - A few practical steps in reviewing/negotiating/renegotiating IT service contracts

Key Elements of Data (really Information) Security Regulations

- Data Breach Notification (reactive, after the fact) 45 States
- Affirmative Information Protection (proactive), a few states (MA, OR, etc.)
- One size fits all in many cases
- Beneficial purposes, but presuppose ample resources (legal, HR, IT, finance, etc.)

The Massachusetts Approach: Harbinger of Things to Come?

- Most Comprehensive Regulatory Scheme among the 45 states to date
- Proactive and reactive (risk minimization, not just damage remediation)
- Prescriptive: detailed administrative, operational, physical and technology mandates
- 450+ pending bills in other State Legislatures

Massachusetts *Standards* as the default template

- Apply to everyone, everywhere where MA residents PII is gathered, stored, licensed, processed or transferred, regardless of overlapping regulations
- Address most likely security lapses –
  - Loss of laptop, flash drive, smart phone, etc.
  - Loss during transfer from office PC to personal device
  - Unauthorized expropriation by former employee or other party
- No generally applicable federal law

Standards: The WISP

Comprehensive written information security program (WISP)

- Administrative and Operational (risk evaluation & responsive policies/practices, delegation, on-going monitoring, training, etc.)
- Physical (safeguarding hardcopy as well as electronic records)
- Technical (encryption in transit, mobile devices as feasible)
- Third Party Vendor Compliance
- All by March 1, 2010

The Standards as they relate to Third Party Vendors of IT Services

- Several actions required –
  - Inventory Contracts, etc.
  - Evaluate Risks
  - Negotiate/renegotiate
  - Monitor Compliance

Selecting and Retaining Third Party Service Providers

- Identify paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information which are in the custody or control of third parties, to determine which records, etc. contain personal information.

Selecting and Retaining Third Party Service Providers

- Proposed revision: 1. Taking reasonable **steps to select and retain** third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and
- 2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that any contract a person has entered into with a third party service provider prior to March 1, 2012, shall be deemed to be in compliance herewith, notwithstanding the absence in any such contract of a requirement that the service provider maintain such protective security measures, so long as the contract was entered into before March 1, 2010.

"Select and Retain"

Four steps ….

(1) Inventory and assess third party contracts, records, systems, etc;

(2) Evaluate capable vendors ["select"] ;

(3) Improve where necessary; and

(4) Monitor performance ["retain"] ….

require all regulated entities to revisit existing long-terms contracts and prepare for renegotiations to bring contracts terms and vendor performance within the ambit of the *Standards*.

“Select” and “Retain” [continued]

Step One:

Identify and catalogue all contracts with third party service providers which may involve PII.

“Select” and “Retain”

Steps Two and Three:

Evaluate the relative vulnerabilities of PII within each existing or proposed contractual arrangement --

a) Indentify and assess type and level of security risks;

b) Evaluate apparent effectiveness of contract-specified or referenced safeguards; and

c) Negotiate/renegotiate “improvements”.

“Select” and “Retain”

Step Four:

- Monitor performance [“retain”]

  Due diligence must be on-going, for the life of the contract or the data
- Any monitoring should be documented
- OCABR’s now abandoned “Certification” requirement still persists, in practical effect

“Select” and “Retain” [continued]

- Really 5 Steps

Step Five:

Document … all the first four steps

“Select” and “Retain” [continued]

Real world questions (i.e. where requisite leverage may be lacking):

- Would contract “reps and warranties” be sufficient? Do you have to audit the representations of the vendor? How? How often?
- How does one compel a long-term or new vendor to (re)open negotiations and to commit to all the detailed administrative, operational, technical and physical security measures (“appropriate” measures)?

What to do?

1. Start with the “riskier” contracts
2. “reps and warranties”, “disclaimers”: review and revise the “boilerplate”
3. Conform SLAs, other vendor undertakings to the *Standards*
4. Your vendor’s negligence may not cover your risks
5. Indemnification (if you can get it)
6. Document, document, document

What to do?

Triage

- Given limited resources and time (and when is this not the case?), deal with the heavier risk laden contracts first, and where leverage is greatest.
- The *Standards* as well as well as most state and federal regulators take into consideration the availability of resources of regulated entities as well as the degree of sensitivity of PII and level of risk.
- Document failed as well as successful efforts to address contract deficiencies with uncooperative vendors.

What to do?

Reps and Warranties

- Assuming the leverage:
  - Expand the “boilerplate” regarding compliance with law to encompass MA, other new regulations
  - Amend “boilerplate” disclaiming “all other” warranties , which conflict with express warranties
  - Document failures as well as successes in achieving reps and warranty reform

What to do?

You're on your own.

- Don’t think vendor’s failure (due to negligence or otherwise) will act to excuse your failure to comply with the *Standards*.
- You cannot delegate liability by contract, but you can try to share the pain (See next slide).
- Your vendor may fail in spite of best efforts, or strict adherence to industry standards.
- “Duty of care” in cyberspace is an elusive concept. Security breaches happen.

What to do?

Indemnification, if you can get it.

- Vendor will (quite reasonably) seek to limit responsibility ("vendor will take commercially reasonable steps" to protect the integrity of data entrusted to it).
- Just as reasonable, you will not want to be the "stuckee", haplessly entrusting your data to the company in the business of safeguarding customer data.

What to do?

Indemnification, continued

- Make sure you're covered for, minimally, vendor's gross negligence.
- Extend the indemnity to all types of third party claims (your customers, data subjects) but also administrative claims from State AG or other enforcement agencies
- Cover remediation costs – notification, free credit reports, etc.)

Enforcement

- Typically the State Attorney General is tasked with enforcing data protection and personal privacy regulations
- OCABR proposes, AG disposes
- Operating with typically vague standards, lack of in-house technical expertise, breadth and depth of AG staff case-by-case enforcement actions hard to gage
- Private right of action – mostly not a threat, yet

Enforcement

- Eventually some “safe harbor” guidelines may evolve, providing some assurance of what passes as acceptable policies and practices
- Worst case scenario: a data breach and no WISP
- Best defense: the WISP, customized to your situation
- New deadline gives 60 more days. Don’t wait to “scramble”

Contact Information

John J. Smith
VistaLaw International LLC
1875 I Street, NW
Fifth Floor
Washington, DC 20006

www.vistalaw.com
202.429.5526 [work]
202.966.9234 [work/home]
202.257.1066 [mobile]