Scrambling for Compliance

Reworking Your Information Technology Service Contracts

Security Camp
Boston University
Boston, MA
August 20, 2009

John J. Smith, VistaLaw International, LLC

Overview of Presentation

- Why “scrambling” ? Why “reworking”?
- 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.)
- Beneficial purposes, but presuppose ample resources (legal, HR, IT, finance, etc.)
- One size fits all

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
- 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)
- Third Party Vendor Compliance
- By January 1, 2010

The *Standards,* a partial summary:

- The regulations establish minimum standards for the protection of personal information. The information security program must:
- Designate one or more employees to maintain the comprehensive information security program;
- Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluate and improve the effectiveness of the current safeguards for limiting such risks, including but not limited to: (i) ongoing employee (including temporary and contract employee) training; (ii) employee compliance with policies and procedures; and (iii) means for detecting and preventing security system failures.
- Develop security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises.
- Impose disciplinary measures for violations of the comprehensive information security program.
- Prevent terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names.
- Take reasonable steps to verify that third-party service providers with access to personal information have the capacity currently in place to protect such personal information.

The *Standards,* a partial summary:

- Limit the amount of personal information collected, the length of time such information is retained, and the access to such information to only that which is reasonably necessary.
- Identify paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information.
- Establish reasonable restrictions on physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted and ensure that such records and data are stored only in locked facilities, storage areas or containers.
- Include regular monitoring to ensure that the program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information and upgrading information safeguards as necessary to limit such risks.
- Review the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.
- Document responsive actions taken in connection with any incident involving a breach of security and conduct a mandatory post-incident review of events and actions taken, if any, to make changes to business practices relating to the protection of personal information resulting from such breach.

[Loeb & Loeb, LLP]

“Verify” and “Insure”

:

Specifically, the *Standards* require -

“verify that any third party service provider with access to personal information has the capacity to protect such personal information …[and] ensure that such third party service provider is applying such personal information security measures at least as stringent as those required [under the *Standards*].

The Standards impose a significant new burden on contracting parties – effectively forcing a renegotiation and likely at some additional cost.

“Verify” and “Ensure” [continued]

A Three step Process:

1. Identify and catalogue all contracts with third party service providers which may involve PII;
2. Evaluate the relative vulnerabilities of PII within each contractual arrangement --
   a) Indentify and assess type and level of security risks;
   b) Evaluate apparent effectiveness of contract-specified or referenced safeguards;(if any); and
   c) Document “a” and “b”
3. Undertake real-time due diligence to determine whether “b” is in effect .

“Verify” and “Ensure” [continued]

- Really 4 Steps?
  - *… and to “ensure that .. provider is applying measures …”*
- Due diligence must be on-going, for the life of the contract or the data
- Any monitoring should be documented
- “Certification” requirement still persists, in practical effect

“Verify” and “Ensure” [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 vendor to reopen negotiations and to commit to all the detailed administrative, operational, technical and physical security measures (“measures at least as stringent as those required [under the *Standards*”])?

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, and in place by year end.

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]