Information Security & Vendor Contracting: Avoiding Common Pitfalls

September 17, 2013

FOLEY

FOLEY & LARDNER LLP

Speakers

Michael R. Overly, Partner, Foley & Lardner LLP

Aaron K. Tantleff, Senior Counsel, Foley & Lardner LLP

3

Agenda and Overview

- Overview of the current landscape of privacy and security laws and regulations.
- Privacy is only part of the problem.
- Identifying three common threads in privacy and security laws and regulations.
- Potential risks of non-compliance.
- Application to vendor contracting process

4

Information Security Risks Are At An All Time High

- In the last year, there were almost a dozen major incidents in which personal information has been severely compromised.
- According to the FBI, incidence of hacking and **insider** misappropriation or compromise of confidential information is at an all time high.
  - Insiders include not only the company's own personnel, but also its contractors and business partners

5

Information Security Risks Are At An All Time High

- FTC, OCC, HHS and other regulators increasingly focusing on information security.
  - States becoming increasingly active in this area.
- Possibility of FTC, AG, and other regulatory action at an all-time high.
- Sanctions can scale to the millions of dollars

6

Biggest Misconceptions

- It's *all* about the data
  - Security of systems
  - Security of data
- It's *all* about privacy
  - Privacy is only a subset of security
  - It's *all* about confidentiality
    - CIA: Confidentiality, Integrity, Availability
    - This requirement is seen in many privacy/security laws and regulations.

7

Examples of Federal & State Laws and Regulations

- Gramm-Leach-Bliley
- HIPAA Security Rule / HITECH Act
- California, Massachusetts, New Jersey, and many others
- Federal Trade Commission

8

Standards

- Australia, US, US State: "Reasonable" measures
- Others: "Appropriate," "necessary" measures
- Contract requirements
  - EU Model Contracts
  - Other Agreements

9

What Are We Protecting

- General Confidential Information
- Intellectual Property
- Protected Health Information (HIPAA)
- Personally Identifiable Non-Public Financial Information (GLB), and other information protected under state privacy and security laws

10

What Are We Protecting

- Other PII, e.g., HR data, investors, business contact information
- System operations
- System integrity

11

Why Protections Are Important

- Protect valuable assets of the business
- Establish due diligence
- Protect business reputation
- Avoid public embarrassment
- Minimize potential liability
- **Regulatory compliance**

12

Three Common Threads

- Attempt to gain a broader picture of compliance obligations.
- Three common themes or “threads”
- Threads run through laws and regulations and, also, common industry standards (PCI DSS, CERT at Carnegie Mellon, and the International Standards Organization)

13

First Common Thread

- Confidentiality, Integrity, and Availability (CIA)
- Foundational principle in information security.
  - Data must be held in confidence
  - Data must be protected against unauthorized modification
  - Data must be available for use when needed

14

Second Common Thread

- Acting "Reasonably" or taking "Appropriate" or "Necessary" measures to protect data
- EU, Australia, Canada, US, and many other countries.
- Business must do what is reasonable or necessary. Perfection is not required.

15

Third Common Thread

- Scaling security measures to reflect nature of data and risk presented.
- Closely related to acting reasonably or doing what is necessary.
- Security measures must be adjusted to reflect the sensitivity of the data and severity of the risk.
- The greater the risk and sensitivity of data, the greater the effort to secure the data.

16

Scaling of Security

- Security isn't an all or nothing proposition.
- Protections must scale to meet the risk.
  - Fees should not be part of the analysis.
- Data security regulations and laws written in terms of scaling.

17

Scaling of Security

- Massachusetts Data Security Law:

". . . safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information."

18

Scaling of Security

- HIPAA Security Rule: Factors to consider:
  - The size, complexity, and capabilities of the Covered Entity.
  - The Covered Entity's technical infrastructure, hardware, and software security capabilities.
  - The costs of security measures.
  - The probability and criticality of potential risks to ePHI.

19

Applying Common Threads to Vendor Contracting Relationships

20

Three Step Approach

- Vendor due diligence
- Contractual protections
- Information handling procedures and requirements, generally in the form of contract exhibits

21

Common Errors

- Failure to involve all relevant stakeholders in the process
- Failing to assess the unique requirements of the transaction at-hand
  - Example: Mobile applications
- Inflexibility

22

Step One: Due Diligence

- From the outset, Vendors must be on notice that the information they provide as part of the company's information security due diligence will be (i) relied upon in making a vendor selection; and (ii) part of the ultimate contract.
- To ensure proper documentation and uniformity in the due diligence process, companies should develop a "Vendor Due Diligence Questionnaire."

23

Step One: Questionnaire Advantages

- Provides a uniform framework for due diligence
- Ensures “apples-to-apples” comparison of vendor responses
- Ensures all key areas of diligence are addressed
- Provides an easy means for incorporating due diligence information into the final contract

24

Step One: Questionnaire Use

- The Questionnaire will address security standards with which Vendors will be required to comply under the laws (e.g, HIPAA, FCRA/FACTA, GLB, etc.). Many Vendors will lack true understanding of these requirements.
- The Questionnaire will be a tool to educate your Vendors about your compliance expectations.

25

Step One: Questionnaire Use

- The Questionnaire should be presented to potential vendors at the earliest possible stage in the relationship.
- Include as part of all relevant RFPs. If no RFP is used, submit to the vendor as a stand-alone document.

26

Step Two: Contractual Protections – Threat Scaling

- NDA or Confidentiality Clause
- General security obligations
- Security and data warranties
- Use of subcontractors/offshore entities
- Personnel controls, diligence

27 Step Two: Contractual Protections

- Breach notification, cost reimbursement
- Indemnity – Protection from third party claims
- Limitation of Liability
- Insurance
- Incorporation of Due Diligence Questionnaire

28 Step Three: Information Handling Requirements

- Where appropriate, attach specific information handling requirements in an exhibit
  - Securing PII
  - Encryption
  - Secure destruction of data
  - Securing of removable media
  - Communication and coordination

29

Negotiation Tips

- Raise security requirements from the outset, including liability expectations
- The way in which the requirements are presented to the vendor is key
- In many cases, it is necessary to educate the vendor about legal/regulatory requirements
- Major push-back to baseline technical requirements is common and almost never difficult to overcome
- Flexibility is frequently required, but generally only for a narrow range of requirements

30

Negotiation Tips

- Create a ready library of "plug-and-play" alternatives to standard required terms
- Addressing the common argument that "we cannot change the way we secure our systems for a single engagement"
- Addressing the argument that baseline security requirements somehow prevent the vendor from evolving its security standards

31

Negotiation Tips

- Moving target language
- "Industry best practices" provisions
- Compliance with laws/regulations that may not directly apply to the vendor's business

32

Post-Execution Follow-up

- Ongoing policing of vendor performance and compliance is crucial
  - Audit rights
  - Access to third party audit reports (e.g., SAS 70 Type II)
  - Updating of due diligence questionnaire is key
- Annual compliance statement

33

Questions?

Please take a moment to complete a short survey about this program.

Click on the link below:
https://www.surveymonkey.com/s/InformationSecurityandVendorContracting

34

Contact Information

Michael R. Overly, Esq.
Partner
CISA, CISSP, CIPP, ISSMP, CRISC
IT & Outsourcing
Foley & Lardner LLP
Tel: 213-972-4533
moverly@foley.com

Aaron K. Tantleff, Esq.
Senior Counsel
IT & Outsourcing
Foley & Lardner LLP
Tel: 312.832.4367
atantleff@foley.com