Strafford

Presenting a live 90-minute webinar with interactive Q&A

Integrating Information Security Protections in Supplier Agreements: Guidance for Business and Technology Counsel

Evaluating Data Security Risks, Negotiating Contractual Protections, Monitoring Supplier Performance

TUESDAY, MAY 25, 2021

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Michael R. Overly, Partner, **Foley & Lardner LLP**, Los Angeles

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-877-447-0294** and enter your **Conference ID and PIN** when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the 'Full Screen' symbol located on the bottom right of the slides. To exit full screen, press the Esc button.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the link to the PDF of the slides for today's program, which is located to the right of the slides, just above the Q&A box.
- The PDF will open a separate tab/window. Print the slides by clicking on the printer icon.

Key Steps For Integrating Information Security Into The Vendor Contracting Process

Michael R. Overly, Esq., CISA, CISSP, COP, CRISC, ISSMP, CIPP
Foley & Lardner LLP

FOLEY
FOLEY & LARDNER LLP

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

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
  - HITECH Interim Rule permits sanctions up to $1.5M

Overview: Information Security

- Security requires a unified approach
  - Security policies
  - Employee education
  - Use of technology (e.g., firewalls, encryption, intrusion detection systems)
  - Security audits
  - Addressing security in contracts with business partners and other vendors

Overview: Information Security

- Security measures can be divided into three categories:
  - Administrative: policies, procedures
  - Technical: firewalls, intrusion detection systems, encryption
  - Physical: secure doors and facilities, video monitoring, security guards.
- Many privacy/security laws and regulations use this very language.

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.

Examples of Federal & State Rules

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

Standards

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

FTC Legal Authority

- Section 5 of the Federal Trade Commission Act ("Section 5") prohibits "unfair or deceptive acts or practices in or affecting commerce."
  - **"Deceptive":** Prohibited practices include deceptive claims that companies make about privacy, including claims about the security they provide for consumer information.
  - **"Unfair":** Requires companies holding sensitive data to have in place reasonable procedures to secure it if the failure to do so is likely to cause substantial consumer injury.

Regulatory Language Should be Treated as a Floor

- Including the HIPAA, GLB, and other statutory/regulatory minimally-required security language, without more, does not adequately protect companies.
- Even the more robust language provided in laws and regulations (e.g., HIPAA Security Rule, GLB Safeguards Rule, etc.) does not provide sufficient protection.
- PCI expressly designed as “floor”

Vendor Contract Protections Not Optional

- Security protections in vendor agreements are required by law:
  - GLB
  - HIPAA/HITECH
  - Massachusetts, California, Maryland, etc.
  - FACTA

Security Best Practices: ISO

- ISO 27001 and ISO 27002/17799:
  "Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements."

CERT Resiliency Management Model

- Manage operational risk, includes three fundamental activities: security, business continuity, and IT operations.
- Managing Relationships with Business Partners to Achieve Operational Resiliency
  - Due diligence
  - Contractual obligations

CERT Definition of "Insider"

- Last year, CERT identified 100+ significant incidents of "insider" breaches.
- CERT recently modified its official definition of "insider" from "current and former employees" to "current and former employees, business partners, and contractors."

FFIEC: Outsourcing Technology Services

- Federal Financial Institutions Examination Council
- IT Examination Handbook assists financial institutions and examiners in evaluating risk management in IT relationships
  - Due diligence
  - Vendor contracting standards
- Excellent reference for every business

Types Of Contracts/Relationships

- When do we need to think about info sec?
- Any agreement under which a third party will have access to the company's:
  - Network
  - Facilities
  - Data
- Access can be remote or physical
- Litmus test

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.

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."

Scaling of Security

- HIPAA Security Rule: Factors to consider:

(i) The size, complexity, and capabilities of the Covered Entity.

(ii) The Covered Entity's technical infrastructure, hardware, and software security capabilities.

(ii) The costs of security measures.

(iv) The probability and criticality of potential risks to ePHI.

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

What Are We Protecting

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

Why Protections Are Important

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

3 Tools for Better Protecting Data Entrusted to Third Parties

FOLEY

FOLEY & LARDNER LLP

Three Step Approach

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

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

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."

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

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.

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.

Step One: Questionnaire Key Areas

- Financial condition
  - Example from ASP and hosting industry
- Insurance coverage
  - Cyber-Crime Coverage
  - Blanket Bond
- Responsibility
  - Criminal convictions
  - Litigation
  - Regulatory enforcement actions
  - Breaches of security, health information
  - Adverse audits
  - Affiliates, Subsidiaries, contractors outside the US

Step One: Questionnaire Key Areas

- Where will the services be performed and data hosted?
  - Don’t neglect help desk providers
- Offshore transmission of data
- Intended use of subcontractors
  - Potential need for further due diligence

Step One: Questionnaire Key Areas

- Personnel Security
  - Screening procedures/Background check
  - Training
  - Ongoing education
  - Termination procedures
- Information Security Policy
  - Electronic communication monitoring

Step One: Questionnaire Key Areas

- Business Continuity/Disaster Recovery
  - Essential to ensuring availability of critical services
  - Understanding of the vendor's plans will also provide valuable due diligence information regarding information security (e.g., where is the recovery site, is the site operated by a third party, how will the data at the site be secured, how will the data be securely transmitted to the site)
  - Security of data at the site impacted by the disaster
- Data destruction procedures

Step One: Questionnaire Key Areas

- Organizational security procedures
  - Information handling policies
  - Dedicated information security team
  - Incident response team
  - Information security practices with contractors and agents
- Physical security procedures
- System access controls – Limiting information access to only those personnel are specifically authorized.

Step One: Questionnaire Key Areas

- Development and Maintenance Procedures
  - Security controls during development lifecycle
  - Security testing
  - Separate environments for testing and production
- Privacy Policy

Step Two: Contractual Protections in Underlying Services Agreement

- NDA or Confidentiality Clause
  - Language should be broadly drafted to include all potential confidential information
- Marking requirements disfavored
- Perpetual protection for NPI
- Ongoing protection of trade secrets
  - Terms on NDAs have been held to limit trade secret protection

Step Two: Contractual Protections

- Standard of care for confidentiality:
  - Vendor shall treat Customer Confidential Information as strictly confidential and shall use the same care to prevent disclosure of such information as it uses with respect to its own most confidential or proprietary information, but in no event less than reasonable care.
  - Vendor shall treat Customer Confidential Information as strictly confidential and shall use the same care to prevent disclosure of such information as it uses with respect to its own most confidential or proprietary information, which shall not be less than the standard of care imposed by state and federal laws and regulations relating to the protection of such information and, in the absence of any legally imposed standard of care, the standard shall be that of a reasonable person under the circumstances.

Step Two: Contractual Protections

- Warranties
  - Compliance with best industry security practices
    - The more stringent of applicable law and regulations or best industry practices
  - HIPAA/HITECH compliance
  - GLB compliance
  - Red Flag/Identity Theft

Step Two: Contractual Protections

- Warranties
  - Other state and federal consumer protection/privacy laws
  - Compliance with Privacy policy
  - Personnel not convicted of crimes of dishonesty
  - Performance of services outside the US
    - Beware support personnel located outside the US
  - Transmission of confidential information outside the US or expressly authorized countries.

Step Two: Contractual Protections

- Vendors who are already subject to outside certifications or regulation
  - Vendors who are "PCI DSS Compliant"
  - Vendors who are ISO 27001/27002 certified
  - Vendors who are regulated entities
    - Consumer reporting Agencies
    - Financial services companies under GLB
    - Covered Entities under HIPAA
    - Business Associates under a Business Associate Agreement
- Certifications and regulatory obligations are an important part of overall protection.

Step Two: Contractual Protections

- Use of subcontractors
  - Strictly limit (exceptions for generic service providers)
  - Approval required
  - Joint and several liability
    - Avoid provisions attempting to prevent actions against suppliers and contractors.
  - Due diligence

Step Two: Contractual Protections

- Use of subcontractors to provide critical functions – hosting providers, outsource partners, etc.
  - Far greater need for due diligence
  - Potential use of a "continuity agreement"
  - Control over changes in these types of critical service providers
    - Ample notice of change
    - Assistance in conducting diligence
    - Termination right

Step Two: Contractual Protections

- For critical subcontractors, consider use of specialized "Subcontractor NDA"
  - Creates privity of contract
  - Ensures subcontractor is on notice of obligations
  - Describes relationship between and among the parties
  - Where appropriate, include specific security requirements in addition to baseline confidentiality

Step Two: Contractual Protections

- Personnel due diligence - Background checks and screening
  - Scope restricted by applicable law
  - Generally never want to receive copies of screening results
  - Reassign personnel who fail required check, without disclosure of names
  - Reserve right in relevant engagements to conduct your own background check for onsite vendor personnel.

Step Two: Contractual Protections

- Control of Personnel
  - Ability to request removal of non-performing personnel or any personnel that present a security threat.
  - Consistency of staff over the term of the project
    - Immediate notice of termination or reassignment.
  - Question vendor about turnover rates, particularly foreign vendors
  - Reserve right to fingerprint and search all items brought into or out of your facilities.
  - Reserve the right to monitor and review all use of your systems by vendor personnel

Step Two: Contractual Protections

- Control of Personnel
  - Compliance with facility access and security policies
  - Vendor identification card
  - Access scheduling
  - Escorts required
- General Audit Provision
  - Permit audit of vendor compliance with contract terms, including confidentiality, security, personnel, etc.
- No Removal of Data

Step Two: Contractual Protections

- General Security Obligations
  - Take all reasonable measures to secure and defend its systems and facilities from unauthorized access or intrusion
  - Periodically test systems and facilities for vulnerabilities
  - Immediate reporting of breaches
  - Joint security audits
  - Regulatory access and compliance
  - Firewalls, antivirus, use of VPNs, on-demand access
- Termination for compliance issues

Step Two: Contractual Protections

- Indemnity -- Protection from third party claims
  - Breach of confidentiality
  - Failure to comply with security requirements
- Exceptions to Limitation of Liability
  - Breach of confidentiality
  - Indemnity
  - Use of name
  - Misappropriation of intellectual property
- Limitations of liability
  - Third party and first party claims

Step Two: Contractual Protections

- Security Breach Notification For PII - - Associated Costs
  - Ensure prompt notice from vendor of potential breach to ensure your ability to comply with applicable laws (i.e., avoiding eleventh hour notices).
  - Control of notice
  - Allocate responsibility for costs to vendor
- Control all other public statements.

Step Two: Contractual Protections

- Insurance
  - Workers Compensation
  - Commercial General Liability
  - Commercial Automobile
  - Commercial Blanket Bond, including Electronic & Computer Crime or Unauthorized Computer Access coverage
  - Professional Liability Insurance (Errors and Omissions)
  - Blanket bond

Step Two: Contractual Protections

- Due Diligence Questionnaire
  - Attach as an exhibit and incorporate into the agreement.
  - Include means to be notified of material modifications to responses.
  - Ensure vendor will not materially reduce the security protections reflected in the Questionnaire.
- Information Handling Requirements (Step Three)
- Annual certification of compliance

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

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

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

Negotiation Tips

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

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

Questions?

Contact Information

Michael R. Overly, Esq., CISA, CISSP, ISSMP, CIPP
Information Technology and Outsourcing Group
Foley & Lardner LLP
555 South Flower Street
Suite 3500
Los Angeles, California 90071
(213) 972-4533
moverly@foley.com

FOLEY
FOLEY & LARDNER LLP