You Will Be Judged By The Company You Keep

Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI

Final Draft for August 2007 CSI Alert

By now most organizations realize that performing information security program reviews or audits of their business partners is a good idea if the partners have been entrusted with sensitive data or access to networks and systems. But performing business partner reviews is more than just a good idea.

- It is a requirement of multiple laws and regulations
- It is typically necessary to demonstrate due diligence
- It may be necessary to comply with contractual requirements
- It can be necessary to comply with your own posted privacy and security policies, depending on how they are worded

A few of the laws that contain legal requirements, either directly or implied, for performing business partner security program reviews include:

- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm Leach Bliley Act (GLBA)
- Sarbanes Oxley (SOX) Act
- Federal Trade Commission (FTC) Act
- Fair and Accurate Credit Transactions Act (FACTA)
- Internal Revenue Code (IRC) Section 7612
- U.S. state breach notice laws
- European Union Data Protection Directive 95/46/EC

While the wording within the laws vary, it is important to know that there is not always a directive explicitly stating, "You must perform a business partner review to be in compliance with this law." However, there are often implications to perform such activities. The regulatory oversight agencies, such as the U.S. Federal Trade Commission (FTC), have made numerous publicized statements to this effect during recent years. I provide some of these statements later in this article.

Many organizations have told me it is very helpful to be able to have the specific passages from the laws and regulations so they can cite the exact requirements. This is also something lawyers tend to appreciate. With this in mind, my objective for this article is not only to indicate the laws and other legal and contractual implications for business partner security reviews, but also to provide excerpts from some of the laws that either explicitly or implicitly require these reviews.

Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule

Most information assurance professionals in the healthcare industry think of HIPAA first when the topic of performing business partner security reviews is raised. The HIPAA requirements for verifying the existence and adequacy of security programs of business partners is found within the Privacy Rule as follows (passages not directly related have been omitted):

> § 164.504 Uses and disclosures: Organizational requirements.
> (e)(1) *Standard: Business associate contracts.*

(2) *Implementation specifications: Business associate contracts.* A contract between the covered entity and a business associate must:
(i) Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:
(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and
(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.
(ii) Provide that the business associate will:
(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;
(B) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;
(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;
(D) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information;
(E) Make available protected health information in accordance with §164.524;
(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;
(G) Make available the information required to provide an accounting of disclosures in accordance with §164.528;
(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and
(I) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

Gramm-Leach-Bliley Act (GLBA) Safeguards Rule
Financial organizations should be familiar by now with the requirements of GLBA. The requirements for verifying the security programs of business partners are found within the Safeguards Rule as follows (passages not directly related have been omitted):

§ 314.4 Elements.
(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
(2) Requiring your service providers by contract to implement and maintain such safeguards.

Sarbanes Oxley (SOX) Act

The topic of what actions must be taken to be in compliance with SOX is interesting and has been hotly debated between many lawyers, auditors and information security professionals. However, multiple guidance documents from the Public Company Accounting Oversight Board (PCAOB), which is the private sector, non-profit organization created by SOX to oversee the auditors of public companies, support verifying the security practices of business partners as part of SOX compliance within several of their documents. For example, PCAOB "Auditing Standard No. 2 – Internal Control" includes the directive:

> "Because of the importance of financially significant locations or business units, the auditor should evaluate management's documentation of and perform tests of controls over all relevant assertions related to significant accounts and disclosures at each financially significant location or business unit, as discussed in paragraphs 83 through 105 [of the standard]."

The referenced disclosures include those made to business partners. The passage from SOX often referenced when considering the security controls, which implies an organization is responsible for evaluating the controls for business partners used in conjunction with financial reporting, follows:

> SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.
> (a) RULES REQUIRED.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—
> (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
> (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

Federal Trade Commission (FTC) Act

Every organization doing business within the U.S. is responsible for following a standard of due care for protecting their customer and business data. This is supported and required by the FTC Act. Jessica Rich, assistant director of the FTC Division of Privacy and Identity Protection, warned within the March 12, 2007 issue of the BNA Privacy & Security Law Report that organizations are responsible for the security of data even when incidents happen while their data is under the care or control of their business partners. "First, the vendor or service provider must comply with the data owning company's internal policy. Second, the vendor must comply with U.S. privacy standards."

A primary goal of the FTC's privacy program is ensuring organizations keep the promises they make to consumers about privacy. This includes consideration of the precautions taken to secure consumers' personal information whether it is within the organization's own facility, or within a business partner's facility.

The FTC has brought many charges against organizations that violate Section 5 of the FTC Act, which prohibits unfair or deceptive practices. Most of these are violations stemming from making promises within a posted website privacy policy and then not having internal policies, procedures, technologies or practices in place to support the promises. The Commission has also used its authority to bring cases against organizations whose information practices cause substantial consumer injury.

The applicable portions of Section 5:

> § 45. Unfair methods of competition unlawful; prevention by Commission (Sec. 5)
> (1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.

Read through the FTC list of cases (URL provided in the next section) and you will see that all organizations are subject to being found guilty of unfair or deceptive acts or practices if they do not have information security in place, not only for their own organization, but also if they do not ensure business partners have proper security practices.

Fair and Accurate Credit Transactions Act (FACTA) Disposal Rule
The Disposal Rule, part of the Fair and Accurate Credit Transactions Act (FACTA) of 2003, requires "people and both large and small organizations that use consumer reports" to take appropriate measures to dispose of sensitive information obtained.

Jessica Rich from the FTC has stated this includes any service providers who handle personal data. Rich said that the FTC will continue to view service providers as integral players in data breaches. Rich stated, "Oversight of service providers and service provider liability should figure prominently in any new data security laws." The FTC has explicitly addressed the failure of service providers to protect data. To see some examples look through the FTC case list at http://www.ftc.gov/os/caselist/index.shtm.

The portions of the FACTA Disposal Rule related to ensuring business partner security follow:

> § 682.3 Proper disposal of consumer information.
> (a) Standard. Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.
> (b) Examples. Reasonable measures to protect against unauthorized access to or use of consumer information in connection with its disposal include the following examples.

These examples are illustrative only and are not exclusive or exhaustive methods for complying with this rule.
(1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed.
(2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed.
(3) After due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material, specifically identified as consumer information, in a manner consistent with this rule. In this context, due diligence could include reviewing an independent audit of the disposal company's operations and/or its compliance with this rule, obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.
(4) For persons or entities who maintain or otherwise possess consumer information through their provision of services directly to a person subject to this part, implementing and monitoring compliance with policies and procedures that protect against unauthorized or unintentional disposal of consumer information, and disposing of such information in accordance with examples (1) and (2) above.

Internal Revenue Code (IRC) Section 7216
IRC section 7216 prohibits anyone who is involved in the preparation of tax returns from knowingly or recklessly disclosing or using the tax-related information provided other than in connection with the preparation of the returns. Those who violate this requirement are subject to a fine and/or imprisonment.

While the regulations under section 7216 provide an exemption for tax return preparers who disclose taxpayer information to a third party for the purpose of having that third party process the return, organizations still need to ensure providers to whom they have entrusted customer PII are aware of this requirement, and that the business partner has appropriate security measure in place to protect the PII.

State breach notice laws
Most of the state privacy breach notice laws, and there are at least 37 of these laws in the U.S., provide no exception for when PII within the possession of a third-party is compromised. So, if a business partner has a privacy breach with the PII from your organization, your organization will generally be responsible. Organizations need to ensure that their contracts contain provisions requiring that business partners provide immediate notification to them of suspected breaches, and allow the organization both to participate in the investigation of incidents and exercise control over decisions regarding external reporting.

International Laws

Data Protection laws in all 25 member states of the European Union must meet the requirements of the EU Data Protection Directive 95/46/EC. One restriction is prohibiting the transfer of PII outside the European Economic Area to countries where there is no protection that is considered as "adequate."

The Directive also requires adequate privacy protection and adequate security measures. These requirements follow the PII to the business partners that have been contracted to provide services for the PII, and the organization that collected the PII is ultimately responsible.

The code within EU Data Protection Directive 95/46/EC that most strongly indicates the need to ensure the security of business partners requires:

> "SECTION VIII
> CONFIDENTIALITY AND SECURITY OF PROCESSING
> Article 16
> Confidentiality of processing
> Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.
> Article 17
> Security of processing
> 1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
> Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
> 2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.
> 3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:
> - the processor shall act only on instructions from the controller,
> - the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.
> 4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form."

Similar requirements exist within the data protection laws of other countries, such as in Canada, Australia, Japan, New Zealand, just to name a few.

Payment Card Industry (PCI) Data Security Standard (DSS)
While the PCI DSS is not a law, this contractually legal requirement generally impacts all organizations that process credit cards. These requirements flow to business partners the card processors contract to handle in any way the credit card data. The text from within PCI DSS that most directly requires business partner security assessments follows:

> 2.4 Hosting providers must protect each entity's hosted environment and data. These providers must meet specific requirements as detailed in Appendix A: "PCI DSS Applicability for Hosting Providers."

Appendix A of PCI DSS states:

> Appendix A: PCI DSS Applicability for Hosting Providers
> Requirement A.1: Hosting providers protect cardholder data environment
> As referenced in Requirement 12.8, all service providers with access to cardholder data (including hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.4 states that hosting providers must protect each entity's hosted environment and data. Therefore, hosting providers must give special consideration to the following:
> A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, as in A.1.1 through A.1.4:
> A.1.1 Ensure that each entity only has access to own cardholder data environment
> A.1.2 Restrict each entity's access and privileges to own cardholder data environment only
> A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10
> A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.
> A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not necessarily guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.

AICPA Ethical Standards
Many professional organizations have obligations for their members. For example, the American Institute of Certified Public Accountants (AICPA) professional ethics division addressed the use of business partners as early as 1973 in Ethics Ruling number 1, under the AICPA Code of Professional Conduct, Rule 301, Computer Processing of Client Returns (ET section 391.001–.002). That ethics ruling specifically deals with using the outside services of business partners to process tax returns. The ruling advises that AICPA members "must take all necessary precautions to be sure the use of outside services does not result in the release of confidential information."

The Code also states that a member remains responsible for ensuring the accuracy and completeness of the services provided by the business partner. Specifically, it requires

all professional services to be performed with professional competence and due professional care. Organizations are responsible for the actions of business partners. Rule 201.01 follows:

> 01 Rule 201—General standards.
> A member shall comply with the following standards and with any interpretations thereof by bodies designated by Council.
> A. Professional Competence. Undertake only those professional services that the member or the member's firm can reasonably expect to be completed with professional competence.
> B. Due Professional Care. Exercise due professional care in the performance of professional services.
> C. Planning and Supervision. Adequately plan and supervise the performance of professional services.
> D. Sufficient Relevant Data. Obtain sufficient relevant data to afford a reasonable basis for conclusions or recommendations in relation to any professional services performed.

Your Organization's Own Promises

The promises your organization makes within posted privacy policies published online or distributed to customers and personnel must be honored. These are legally binding documents. As mentioned earlier, if you do not keep your promises your organization can be accused of unfair and deceptive business practices under the FTC Act. Look at your contracts and your website privacy policies. If you state something such as, "Company X has policies and procedures in place to limit access to your information to only those who have a business need to view it," then you may have legally obligated yourself to perform business partner security program reviews to back up this statement. Talk with your legal counsel about this.

Action Items

As you can see, information privacy and security laws impose many obligations upon organizations that entrust PII to business partners to verify the security of those business partner security practices. Organizations need to incorporate due diligence actions within the procedures used to contract business partners to handle, process or otherwise access PII to meet these obligations.

I have been performing business partner security reviews for the past several years, and I have created a methodology based upon using ISO 17799:2005 (now ISO 27002) and the OECD privacy principles. Consider using these documents to help you do a comprehensive review. Along with these consider the following as a starting point for you to create your own business partner security review procedures. As always, be sure to discuss these activities with your legal counsel to help identify which ones would be most appropriate for your own organization, and which ones would either not be applicable or be necessary based upon your business environment.

- Contractually limit business partner use of PII to only the purposes for which the PII was provided.
- Do not allow PII to be used for application testing or piloting purposes.
- Do not allow business partners to subcontract PII handling or access activities without your organization's explicit knowledge and approval.

- Ensure your business partner has an incident response plan and privacy breach notice procedure that includes your organization as soon as the incident is identified.
- Review business partner information security and privacy policies to ensure they are appropriate and comprehensive.
- Ensure your business partner provides good and ongoing information security training and awareness communications to their personnel who handle or access your organization's PII.
- Periodically require an independent third party review of the business partner's security program.
- Include detailed information security and privacy requirements within the contracts your organization has with business partners.
- Establish procedures to oversee the business partner's use of the PII you provided to them.
- Ensure your business partners are in compliance with applicable data protection laws and regulations.
- Include a provision within your business partner contract that violation of the security requirements can result in immediate termination of the contract.
- Discuss with your legal counsel how your organization will handle a situation in which a business partner suffers a privacy breach for the PII from your organization. If the involved individuals bring a suit or win a judgment, what responsibility will the business partner have for compensation? How can this be contractually enforced?
- Remember that PII must be safeguarded anywhere in the world where it is located; don't limit your due diligence activities to just the county where your organization is based if you have customers and/or business partners outside your country.
- Do careful research to know your business partner. Identify any lawsuits or incidents in which they have been involved.

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor. Her latest publications are Say What You Do (Shaser-Vartan) and The Privacy Management Toolkit (Information Shield). She can be reached at rebeccaherold@rebeccaherold.com or http://www.privacyguidance.com.