Cybersecurity Standards and Risk Assessments for Law Offices: Weighing the Security Risks and Safeguarding Against Cyber Threats

David Z. Bodenheimer and Cheryl A. Falvey*

I. Introduction

Why have law offices become significant targets of cyber attacks? In short, law offices house some of the world's most valuable secrets. These secrets cut across virtually every legal practice area, imposing duties upon lawyers in both the public and private sectors to protect the confidentiality of such data. At a glance, such secrets include the following:

- Trade Secrets. Private litigators and government regulators handle commercial data and trade secrets of extraordinary value.[1]
- Corporate Deals. Corporate lawyers and antitrust regulators work on huge mergers and acquisitions involving highly confidential data.
- Personal Data. A wide spectrum of lawyers have access to very sensitive personal data – *e.g.,* class-action litigators, tax attorneys, and employee-benefits practitioners.
- Export-Controlled Technology. Law offices ranging from the U.S. State Department to private international law practices review data subject to strict export controls.
- Healthcare Information. Lawyers in both the public and private sectors handle highly sensitive health care information.

And of course attorney-client privileges and attorney work product represent some of the most important and sensitive secrets in the practice of law.

---

*David Z. Bodenheimer, a partner in Crowell & Moring LLP's Washington, DC office, specializes in Government Contracts and heads the Homeland Security practice. He currently serves as ABA Science & Technology Law (SciTech) Division Chair (Security, Privacy, and Information Law), Committee Chair (Homeland Security), and Public Contract Law Section (PCL) Committee Co-Chair (Cybersecurity, Privacy, and Data Protection Committee). Cheryl Falvey previously served as General Counsel for the Consumer Product Safety Commission and currently is a partner in Crowell & Moring's Washington, D.C. office where she co-chairs the firm's Advertising & Product Risk Management Group. Special thanks are due to our colleagues – Kerry Mustico, Elliot Golding, Kate Molony and Gordon Griffin – for their key contributions.

[1] *See, e.g., Ruckelshaus v. Monsanto,* 467 U.S. 986 (1984) (unauthorized disclosure of trade secret data in course of regulatory process).

How pervasive are cyber threats to law offices? The risks are not easy to quantify given that law offices tend to underreport cybersecurity vulnerabilities and breaches.[2] Even with apparent underreporting, Mandiant reported that 80 law firms had been hacked in 2011 alone.[3] The scope and gravity of the breaches of law firms continues to be sobering:

> Most major U.S. law firms have been victims of security breaches, and the unwelcome threats likely operated covertly for up to nine months before they were discovered. For many, the first whiff of insidious action comes from a knock on the firm's door by the FBI.[4]

Increasingly, hackers have looked to law firms as a backdoor into their clients' most valuable secrets. As the Assistant General Counsel of Bank of America warned, law firms are "'considered one of the biggest vectors that the hackers, or others, are going to go at to try to get to our information.'"[5] One of the more widely reported security breaches occurred in the midst of an unsuccessful attempt to close a $40 billion corporate acquisition:

> China-based cyber thieves, for instance, hacked into the computer networks of seven law firms in 2010 to get more information about BHP Billiton Ltd.'s ultimately unsuccessful $40 billion bid to acquire Canadian company Potash Corp. of Saskatchewan, Inc., Bloomberg reported in January.[6]

Given such escalating risks to law offices, ABA President Laurel Bellows has made law firm cybersecurity a priority for 2012-13.[7] Based upon the magnitude of the risks and the recognized ethical obligations, hardly anyone would argue that lawyers need not worry about cybersecurity. The more difficult question is what

---

2 Jennifer Smith, "Lawyers Get Vigilant on Cybersecurity," *Wall Street Journal* (June 26, 2012) (quoting former FBI agent and Executive Assistant Director Shawn Henry).

3 Martha Neil, "Corporate Clients Should Ask Specific Questions About Law Firm Computer Security, Experts Say," *ABA Journal* (Feb. 21, 2012) (citing Michael Riley & Sophia Pearson, "China-Based Hackers Target Law Firms to Get Secret Deal Data," *Bloomberg Businessweek* (Feb. 8, 2012)).

4 Rachel M. Zahorsky, "Being Insecure: Firms are at Risk Inside and Out," *ABA Journal* at 32 (June 2013).

5 Catherine Dunn, "Outside Law Firm Cybersecurity Under Scrutiny," *Corporate Counsel* (June 6, 2013) (quoting Richard Borden, Assistant General Counsel, Bank of America).

6 Elgin, Lawrence & Riley, "Coke Gets Hacked and Doesn't Tell Anyone," *Bloomberg.com* (Nov. 4, 2012) (http://www.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-t-tell.html).

7 James Podgers, "Raising the Alarm," *ABA Journal* at 55 (Feb. 2013).

lawyers should do about it. A number of books and articles have provided guidance and recommended best practices for law firm cybersecurity, including several works by the ABA.[8]

This discussion focuses upon two key elements that law offices should consider in implementing a sound cybersecurity program:

(1) why law firms should perform a risk assessment; and

(2) what are the applicable standards governing cybersecurity?

Neither the ABA guidelines nor the general ethical opinions provide specifics on cybersecurity risk assessments and standards. While this discussion does not identify a particular risk assessment methodology or information security standard as the right one for every law office, it does seek to inform lawyers of the choices that should be made in tailoring an information security program for the specific risks, data, and security needs that law offices face in their daily practices.

II. Risk Assessments for Law Offices

A risk assessment represents a critical first step for a sound information security program. While a variety of information security standards exist in the public and private sectors, nearly all include a risk assessment as an essential building block in the security process. Furthermore, a risk assessment serves important practical functions in getting the most bang for the buck.

A. Risk Assessments as Part of a Cybersecurity Program

As a rule, information security standards include a risk assessment as a way to identify the primary risks and vulnerabilities and focus the strongest defenses against the biggest risks. For example, the Securities and Exchange Commission (SEC) issued cybersecurity guidance for publicly traded companies and identified the need for risk assessments for cyber threats:

> Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky. [footnote omitted] In determining whether risk factor disclosure is required, we expect registrants to **evaluate their cybersecurity risks and take into account all available relevant information**, including prior cyber incidents and the severity and frequency of those incidents. As part of this evaluation, registrants should consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks,

---

[8] For example, *see* Sharon D. Nelson, John W. Simek, & David G. Ries, *Locked Down: Information Security for Lawyers* (ABA Section of Law Practice Management, 2012); Judge Herbert B. Dixon, Jr., "Cybersecurity . . . How Important Is It," *The Judges' Journal* at 36 (Fall 2012).

> including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption. In evaluating whether risk factor disclosure should be provided, registrants should also consider the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware.[9]

In this guidance, the SEC notes that cybersecurity risks apply not only to publicly traded companies, but also "their business partners."[10] For this reason alone, law firms working with publicly traded companies may find risk assessments to be helpful in aligning their cybersecurity practices with their clients' approach to protecting essential corporate secrets.

Similarly, the NIST information security standards include risk assessments as a fundamental component of a cybersecurity program.[11] In its standards, NIST lays out a six-step framework for a structured risk assessment. For law offices, some of the relevant considerations may include the following:

- What are your information technology (IT) network boundaries? If you have many offices spread across international boundaries with many devices (laptops, tablets, smartphones, and devices from home), you have bigger risks and need more robust security defenses.

- What data do you store and exchange? If your office is handling the Coca Cola formula, for example, it needs more security than it does for the plans outlining the office picnic.

- Who is inside your network boundary? If you have business partners or contract attorneys with direct access to your internal network, you have a greater insider threat than a system limited to your law office members.

- What are your security controls? With bigger risks, you will need more layers of more robust security controls.

- Are your risks static? Of course not. As the risks escalate and shift over time, your cybersecurity controls must adapt to the changing threat environment.

---

9 SEC, *Cybersecurity: CF Disclosure Guidance: Topic No.* 2 (Oct. 13, 2011), at 3 (emphasis added), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

10 *Id.* at 2.

11 NIST Special Publication (SP) 800-39, *Managing Information Security Risk* (Mar. 2011); NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (Feb. 2010).

While just a summary of the much more detailed NIST standards for a risk management framework, these factors should be informative in tailoring a cybersecurity program to the specific needs, risks, data, networks, and other factors that drive the size, shape, and complexity of a law office's cybersecurity defenses.

These NIST standards for a risk management framework serve as a useful source, in part, because NIST seeks to harmonize its guidance with both commercial and international standards.[12] Examples in the risk management arena include the following International Standards Organization (ISO) standards:

- ISO/IEC 31000, *Risk management – Principles and guidelines;*
- ISO/IEC 31010, *Risk management – Risk assessment techniques;*
- ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements; and*
- ISO/IEC 27005, *Information technology – Security techniques – Information security risk management systems.*

B. Practical Reasons for Performing a Security Risk Assessment

Risk assessments not only are an accepted component of a good information security program, but also may have practical benefits to law offices. Given that law offices (like everyone else) have finite resources to deploy, a risk assessment helps to focus security safeguards where they can do the most good with greatest efficiency.

Risk-Based Security. By "assessing the risk and magnitude of the harm that could result,"[13] an organization can determine what – and how much – security it needs. Given that the prevailing standard is reasonable or acceptable security (not perfect security), a risk assessment provides a tool to balance the level of security needed against the magnitude of the risks.[14]

Flexibility. Different law offices have different risk profiles that require different security safeguards. To account for such differences among organizations, the NIST standards emphasize "flexibility" by allowing "different security solutions that are equally acceptable" and that can be tailored to a particular entity's needs.[15]

---

12 NIST SP 800-39, at 4 (Mar. 2011).

13 44 U.S.C. § 3544(a)(2)(A).

14 *See, e.g.,* Federal Acquisition Circular 2005-06, 70 Fed. Reg. 57450-51 (2005) ("information security protections" must be "commensurate with security risks").

15 NIST SP 800-37, at iv, n.3 (Feb. 2010).

Cost-Effective Safeguards. Reasonable security does not mean security at any cost. Some information security regimes expressly recognize cost-effectiveness as part of the risk assessment framework.[16] Given this factor, law offices can tailor their security budgets to the level of risk, thus applying resources more efficiently.

In summary, a risk assessment has real practical value to law firms by: (1) allowing lawyers to justify the level of security based upon the threat levels; (2) deploying the right security safeguards against the most pressing risks; and (3) recognizing that security investments should be cost-effective.

III. Information Security Standards for Law Offices

At present, lawyers operate under a standard of reasonable security for information held in law offices.[17] However, the ABA guidance and state ethical canons do not specify detailed cybersecurity standards defining what particular security procedures, controls, and technology constitute "reasonable" security for lawyers. No single security checklist exists for all law offices for a simple reason – a single "one-size-fits-all" standard could hardly address the kaleidoscope of risks, data, practices, technology, and security needs of every small, medium, and large law office in the public and private sectors.

On the other hand, the standard of reasonable security leaves much room for dispute. When a security breach occurs, a law office may prefer not to leave so much to the imagination of angry clients, litigious parties, politicized Congressional hearings, and/or unsympathetic judges. While the cybersecurity standards below only apply in certain circumstances, they serve three purposes: (1) informing law office management about some of the more common security standards; (2) providing some objective benchmarks against which law offices may measure their cybersecurity programs; and (3) illustrating commonality among the various standards.

A. Public Sector Information Security Standards

If viewed as a whole, the federal government would presumably boast the world's largest law firm.[18] Like their agencies, these public sector lawyers operate under a statutory information security standard imposed by the Federal Information Security Management Act (FISMA).[19] Furthermore, this statutory standard applies to many government contractors, thus extending its sphere over a portion of the private sector.[20]

---

16 44 U.S.C. § 3544 ("implementing policies and procedures to cost-effectively reduce risks to an acceptable level"); NIST SP 800-37, Rev. 1, at 2 ("cost effective, risk-based decisions").

17 *See, e.g.,* David G. Ries, "Cyber Security for Attorneys: Understanding the Ethical Obligations," *LawPractice Today* (Mar. 2012) (www.lawpracticetoday.org).

18 In 2011, federal jobs accounted for nearly 115,000 legal positions in executive and independent agencies. NALP and PSLawNet, *2011-2012 Federal Legal Employment Opportunities Guide* at 5, http://www.law.asu.edu/LinkClick.aspx?fileticket=bfNbH9KWjsY%3D&tabid=1136.

19 44 U.S.C. §§ 3541-49.

20 44 U.S.C. § 3544(a) and (b).

The statute itself includes some general standards for information security, such as requirements for security procedures, policies, controls, monitoring, incident response, and continuity of operations.[21] The detailed implementation of the FISMA security standards, however, may be found in guidance issued by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).[22]

While the NIST information security standards do not expressly apply to law firms or lawyers, NIST continues to gain traction not only in setting standards in the public sector, but also in establishing a cybersecurity framework for critical infrastructure under President Obama's cybersecurity executive order issued in February 2013.[23] For these reasons, law offices may find the NIST standards to be instructive in deciding how to structure an information security program.

1. Establishing Security Objectives

Information security serves three objectives: protecting the confidentiality, integrity, and availability of information. These terms are defined by statute and regulation.

> Confidentiality "means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information."
>
> Integrity "means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity."
>
> Availability "means ensuring timely and reliable access to and use of information."[24]

Confidentiality. Every information security standard includes confidentiality as an essential objective. Lawyers understand the obligation of confidentiality, because protecting client confidences has long been at the core of the attorney-client privilege.

Integrity. In the era of electronic records, an undetected alteration of records (*e.g.,* spoliation due to unauthorized deletion of records) could have a devastating impact on data integrity. Similarly, the integrity of a law firm's trust accounts may be compromised by a cyber attack, as happened when hackers stole "a large six

---

21 44 U.S.C. § 3544.

22 44 U.S.C. § 3544; 40 U.S.C. § 11331(b)(1)(C).

23 Exec. Order No. 13,636, 78 Fed. Reg. 11739, 11742 (Feb. 19, 2013).

24 44 U.S.C. § 3542(b)(1); *see also* Federal Acquisition Regulation (FAR) § 2.101 (defining terms as part of "information security").

figure" sum from a firm's trust account.[25] To maintain the integrity of their data, law offices need sufficient security safeguards not only to prevent such attacks, but also to detect such penetrations and correct unauthorized alterations.

Availability. Terrorist attacks and natural disasters have underscored the importance of back-up systems to assure ready availability of data. Similarly, an attack by international hackers known as Anonymous brought down a law firm's website and resulted in its web host's servers being "wiped clean of all client email."[26] To assure availability of data, law offices need not only a continuity of operations plan, but also built-in resilience to bring the networks back up quickly.

2. Identifying Security Needs

The best security systems are planned. The FISMA statutory requirements, OMB guidelines, and NIST standards lay out the key steps for identifying what the organization needs and how to structure the security program. In a nutshell, some of the most important planning functions include the following:

- System Boundaries. To secure an information system, you need to know what is in it – what offices, people and devices. The security planning must define the boundaries of the information network, systems, and devices to be secured.[27]

- Data Mapping. To tailor security safeguards to the data, you need to know what data you have – and where it goes. The security planning includes a determination of what data the organization holds, the risks relating to such data, and the impact of losing the data.[28]

- Applicable Requirements. Different data may entail different legal requirements (*e.g.,* healthcare information, sensitive personal data, export-controlled technology, *etc.*). For such data, the federal standards include an assessment of what requirements apply to what data.[29]

---

[25] Yamri Taddese, "Law firm's trust account hacked, 'large six figure' taken," *Lawtimesnews.com* (Jan. 7, 2013).

[26] Martha Neil, "Unaware 'Anonymous' Existed Until Friday, Partner of Hacked Law Firm Is Now Fielding FBI Phone Calls," *ABA Journal* (Feb. 6, 2012); *see also* Scott Shane, "F.B.I. Admits Hacker Group's Eavesdropping," *New York Times* (Feb. 3, 2012) (law firm website defaced and then taken down).

[27] NIST SP 800-37, Rev. 1, at 10 (Feb. 2010).

[28] *Id.,* at 7 *citing* NIST Federal Information Processing Standards Publication (FIPS PUB) 199 (Feb. 2004).

[29] *See, e.g.,* 44 U.S.C. § 3544(a)(3)(C) ("policies, procedures, and control techniques" must "address all applicable requirements").

- Risk Assessment. As discussed above, a risk assessment is an essential step in planning and identifying cost-effective safeguards tailored to the particular risk profile of your organization.

In today's world, security planning is not a one-time event because the cyber threats shift and morph with speed of electrons. As a result, the public sector security approach has moved from annual checkups and updates to a continuous monitoring security model.[30] To oversimplify, continuous monitoring involves a six-step process:

- Define a strategy that reflects your office's risk tolerance based upon the latest vulnerabilities and threats and the impact to your business (*i.e.,* likelihood and harm from a security breach).

- Establish a security program that uses metrics and frequent monitoring to check the effectiveness of your security controls.

- Implement the security program by collecting security and threat data and automating the data collection, analysis, and reporting as much as possible.

- Analyze the security and threat data to see how security controls should be revised, fixed, or redeployed.

- Respond to security reports by fixing the security system and/or mitigating the damage.

- Review and update the monitoring program and security defenses to address the latest threats and vulnerabilities.

Continuous monitoring allows an organization to respond quickly to changing threats. For example, if the monitoring system picks up a sudden spike in cyber attacks from North Korea, the security team gets the report in real-time, develops a rapid fix (*e.g.,* blocking email traffic from North Korea), and then checks whether the fix worked. With this process, some federal agencies have reported significantly improved security with greater cost-effectiveness than the prior model of reviewing and updating security strategies and controls on a fixed annual schedule.

3. Implementing a Security Program

After security planning comes implementation of the security program. FISMA's statutory requirements identify a number of top-level elements of a security program, including security policies, procedures, controls,

---

[30] NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (Sept. 2011).

and configuration requirements.[31] The NIST standards include voluminous detail and numerous controls for such security programs.[32] Some of the more salient features of a security program include the following:

- Policies & Procedures. While some may dismiss security policies and procedures as a paperwork exercise, the prevailing security standards (including FISMA) require them.[33] Policies and procedures serve a valuable function (in conjunction with training) of communicating who is responsible for what, when, and why.

- Security Controls. The FISMA requirements and NIST standards specify "management, operational, and technical controls" to safeguard information,[34] ranging from software controls (anti-virus software) to people controls (who can access what and how). By including operational and management controls, these standards underscore the fact that information security must involve the entire organization, not just the IT department's focus on technical controls.

- Configuration Controls. Configuration requirements represent another key element of an information security program.[35] Such configuration requirements include not only assessing changes and limiting unauthorized modifications (*e.g.,* installing a screen-saver that contains a virus), but updating security controls to address new threats.

- Continuity of Operations. A security program must include a plan to continue operations after a disaster or attack.[36] Typical elements include off-site data backup systems and procedures for alternate access to the network.

4. Ensuring Compliance

Once the security program is implemented, it must be enforced. Again, the FISMA statutory requirements expressly include such elements as training, testing, incident detection and reporting, and

---

31 44 U.S.C. § 3544.

32 NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013).

33 44 U.S.C. § 3544(a)(2)(C).

34 *See, e.g.,* 44 U.S.C. § 3544(b)(5); NIST SP 800-53, Rev. 4 (Apr. 2013).

35 *See, e.g.,* 44 U.S.C. § 3544(b)(2)(D); NIST SP 800-53, Rev. 4 (Apr. 2013).

36 44 U.S.C. § 3544(b)(8).

remedial actions.[37] The NIST standards contain extensive detail for enforcing the security program.[38] Some of the key elements include the following.

- Training. Training is not only required,[39] but essential to an effective security program. Many security threats inflict injury not due to a gap in the technical controls, but because of social engineering (*e.g.,* someone clicked on a bad website and brought back a virus).

- Monitoring. The security program must be tested, monitored, and updated for security threats.[40] As discussed above, continuous monitoring involves a real-time monitoring and updating process to defend against rapidly evolving and escalating threats.

- Accountability. A security program requires that personnel must be held accountable for following the security rules.[41]

- Incident Detection and Reporting. When the security defenses are breached, an organization must have a way to detect the breach and a method for reporting it.[42]

B. Health Care Information Security Standards

Law firms that encounter healthcare information may be subject to additional security and privacy requirements under the Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH Act).[43] The Department of Health and Human Services (HHS) has issued regulations implementing the provisions of these statutes: the Privacy Rule, the Security Rule, and the Breach Notification Rule.[44] HHS recently finalized these regulations in an Omnibus Final Rule in January 2013.[45] Within HHS, the Office of Civil Rights has responsibility for implementing and enforcing the Privacy, Security, and Breach Notification Rules issued pursuant to HIPAA and the HITECH Act provisions.

---

37 44 U.S.C. § 3544.

38 NIST SP 800-53, Rev. 4 (Apr. 2013).

39 44 U.S.C. § 3544(b)(4).

40 44 U.S.C. § 3544(a)(2)(D).

41 44 U.S.C. § 3544(a)(3)(A).

42 44 U.S.C. § 3544(b)(7).

43 *See* Pub. L. No. 104-191 (HIPAA) and Pub. L. No. 111-5 (HITECH).

44 *See* 45 C.F.R. Part 160 and Subparts A-E of Part 164 (implementing regulations).

45 *See* 78 Fed. Reg. 5566 (Jan. 25, 2013).

1. Protecting Privacy (HIPAA Privacy Rule)

The Privacy Rule sets a federal minimum for the protection of "Protected Health Information" (PHI), which refers to health information about an individual's physical/mental health or conditions, the provision of healthcare to the individual, or payment for healthcare that can be used to identify a specific individual. Common identifiers include name, address, birth date, and Social Security number.[46] The Privacy Rule seeks to ensure that PHI is protected while allowing the necessary flow of health information to promote high quality health care.

The Privacy Rule applies to "Covered Entities" (CE) and, to a lesser extent, "Business Associates" (BA). CEs are health care providers, group health plans, and healthcare clearinghouses. With limited exceptions, BAs are entities that create, receive, maintain, or transmit PHI on behalf of a CE.

Much of the Privacy Rule sets forth rules regarding the use and disclosure of PHI. The Privacy Rule bars covered entities and business associates from using or disclosing PHI, unless the rule sets forth an exception.[47] Some uses and disclosures are permissible if an individual provides consent. The Privacy Rule also describes several permitted uses and disclosures for which individual consent is not required. The three main "permitted" uses and disclosures are for treatment,[48] payment,[49] and healthcare operations.[50] Other uses and disclosures are required, such as disclosures requested by the Secretary or as otherwise required by law. Disclosures to BAs are also permissible so long as the covered entity enters into a "business associate agreement" (BAA) that requires the BA to have adequate security and delineates the permissible uses and disclosures.[51] In most circumstances, CEs and BAs must make reasonable efforts to limit PHI to the "minimum necessary" to accomplish the intended purpose of the use, disclosure, or request.[52]

The Privacy Rule also sets forth a number of individual rights regarding PHI. With certain limitations, these rights include access (a right to inspect and receive a copy of PHI);[53]amendment (a right to amend PHI);[54] and an accounting of external disclosures (a right to know whether and to whom PHI has been disclosed).[55]

---

46 The Rule does not apply to "de-identified" health information, which is information that does not identify an individual or permit identification. Information that has been de-identified is no longer considered to be PHI. 45 C.F.R. § 164.514(a).

47 45 C.F.R. § 164.502(a).

48 *See* 45 C.F.R. § 164.506(c)(1) and (2); *see* 45 C.F.R. § 164.501 (defining treatment).

49 *See* 45 C.F.R. § 164.506(c)(3); *see* 45 C.F.R. § 164.501 (defining payment).

50 *See* 45 C.F.R. § 164.506(c)(4); *see* 45 C.F.R. § 164.501 (defining healthcare operations).

51 45 C.F.R. § 164.504(e).

52 *See* 45 C.F.R. §§ 164.502(b), 164.514(d).

53 45 C.F.R. § 164.524.

Finally, the Privacy Rule imposes administrative requirements to ensure compliance, including: (1) establishing appropriate policies for the use and disclosure of PHI; (2) designating a privacy official; (3) implementing administrative, technical, and physical safeguards to protect the privacy of PHI; (4) training and disciplining the workforce (including applying appropriate sanctions for failure to comply with policies and procedures); and (5) mitigating the adverse impact of wrongful use or disclosure of PHI.[56]

2. Protecting Security (HIPAA Security Rule)

BAs and CEs must implement "reasonable and appropriate administrative, technical, and physical safeguards" to ensure the integrity and confidentiality of PHI and protect against "reasonably anticipated" threats and unauthorized uses and disclosures.[57] The Security Rule is intended to be flexible and technology-neutral to enable information security levels to be proportionate to the types of threats and the covered entity's circumstances (including size, infrastructure, and security costs).[58] The Security Rule contains numerous "Standards" with which covered entities and business associates must comply.[59] Many of these Standards are accompanied by more specific "Implementation Specifications" reflecting two categories of controls – mandatory ("Required") and potentially applicable ("Addressable").[60]

First, the Security Rule requires sufficient "administrative" safeguards, which seek to ensure that risks are identified and that people implement the safeguards.[61] Administrative safeguards include conducting a risk analysis, training employees, and responding to and reporting security incidents.

Second, the Security Rule requires physical safeguards, which target the physical storage of PHI.[62] These safeguards include facility access controls, policies regarding workstation use and security, and implementing controls surrounding devices and media, including disposal.

(continued…)

54 45 C.F.R. § 164.526.

55 45 C.F.R. § 164.528(a).

56 *See* 45 C.F.R. § 164.530.

57 42 U.S.C.A. § 1320d-2(d).

58 45 C.F.R. § 164.306.

59 45 C.F.R. § 164.306(c).

60 45 C.F.R. § 164.306(d).

61 45 C.F.R. § 164.308.

62 45 C.F.R. § 164.310.

Third, technical safeguards are required, which largely relate to IT security.[63] Such safeguards include access controls (such as user names and passwords), encryption or other forms of data protection, audits, and other authentication measures.

Finally, the Security Rule has several "organizational" requirements as well as "policy and procedure" requirements, which require written business associate agreements, sufficient documentation, and periodic reviewing and updating of policies and procedures.[64] The Privacy Rule contains related standards that require covered entities and business associates to ensure that downstream contractors protect PHI, report security incidents, and cure any material breaches of the BA agreement.

3. Providing Notification of Security Breaches

The HITECH Act introduced a minimum national standard for providing notification for security breaches involving PHI. Under the prior Interim Final Rule, covered entities had greater flexibility in determining whether breach notification would be required, as HHS only required notification if there was a "***significant*** risk of financial, reputational, or other harm to the individual." HHS eliminated the more subjective "risk of harm" standard in the Final Rule in favor of a presumption that any impermissible use or disclosure constitutes a breach.[65] Thus, the new risk assessment standard focuses on whether unauthorized recipients have accessed or had the opportunity to access PHI, rather than the risk of harm to an individual.

The Breach Notification Rule sets forth specific timing, methods, and content for breach notification. Breach notification must occur "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach."[66] Notification to the individual usually must be provided via first class mail. HHS must be notified and, in some cases, the media must be notified of a breach. The notification must provide a brief description of what happened (*e.g.,* dates of breach and discovery), the types of data involved, any mitigation efforts that are being undertaken, information for how individuals can protect themselves, and contact information.[67]

4. Enforcing HIPAA (Sanctions and Penalties)

The Omnibus Rule finalized the liability structure for HIPAA violations. The civil monetary penalties (CMP) increase with the degree of culpability by the covered entity or business associate.[68]

---

63 45 C.F.R. § 164.312.

64 45 C.F.R. § 164.314-316.

65 45 C.F.R. § 164.402.

66 42 U.S.C.A. § 17932(d); 45 C.F.R. § 164.404(b).

67 42 U.S.C.A. § 17932(f); 45 C.F.R. § 164.404(c).

68 42 U.S.C.A. § 1320d-5(a)(3); *see* 45 C.F.R. § 160.404(b)(2).

TABLE 2—CATEGORIES OF VIOLATIONS AND RESPECTIVE PENALTY AMOUNTS AVAILABLE		
Violation category—Section 1176(a)(1)	Each violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	$100–$50,000	$1,500,000
(B) Reasonable Cause	1,000–50,000	1,500,000
(C)(i) Willful Neglect-Corrected	10,000–50,000	1,500,000
(C)(ii) Willful Neglect-Not Corrected	50,000	1,500,000

The precise fine will depend on factors such as the nature and extent of the violation (including the number of persons affected and time period during which the violation occurred), the nature and extent of the resulting harm, the history of prior compliance with the provision, the financial condition of the covered entity or business associate, and "such other matters as justice may require."[69]

The Secretary may impose a separate fine for each provision that is violated and to treat the violation of a single provision affecting multiple people or that is ongoing as multiple violations.[70] The Secretary may aggregate fines for each violation of a single provision within a calendar year, subject to a cap of $1.5 million that applies separately to each distinct HIPAA provision. HHS has suggested that, depending on the nature of the violation, a separate fine may apply on a per-person basis or a per-day basis.

OCR has entered into several large settlement agreements for alleged HIPAA violations in recent years involving organizations of all sizes. The breach reporting requirement often triggers a more extensive OCR audit that identifies additional HIPAA violations. The largest settlements have involved failing to implement adequate policies and procedures to safeguard PHI, to train employees sufficiently, to encrypt devices and other media, and to conduct proper risk assessments.

In addition to OCR enforcement actions, State Attorneys General may also pursue enforcement actions for HIPAA violations. Attorneys General may seek statutory damages for up to $100 per violation, subject to an annual cap of $25,000 for multiple violations of a single HIPAA provision.[71]

C. State Security Breach Standards

Nearly every state has enacted some version of a security breach notification law with varying requirements and different scopes. Some state laws focus more on protecting against identity theft and financial loss, while others limit the application of such laws to entities that are most likely to process large volumes of personal information. Other states have very broad privacy protections, like in Europe, that cover every type of person or entity, without exclusion for those already subject to sector-specific federal privacy statutes and regulations.

---

69 45 C.F.R. § 160.408

70 45 C.F.R. § 160.406

71 42 U.S.C.A. § 1320d-5(d)(2).

1. State Breach Notification Laws

In general, state security breach notification laws require notification to individuals for a breach involving "personal information." "Person Information" typically refers to an individual's first name or initial and last name ***plus***: his or her social security number; driver's license number or other state ID number; or account number, credit or debit number plus security code, access code, or password. Some states include broader definitions of personal information, such as Arkansas (which includes medical information in combination with name) or North Dakota (which includes a mother's maiden name).

Other variations include:

- Time Period. Although some states set specific time periods in which notification must be provided (generally 45-60 days), many states more generically require notification "as soon as possible" or "without unreasonable delay." Some states have even shorter windows. California, for example, recommends providing notification within 10 days.

- Harm Trigger. Many states only require notification if there is a "risk of harm," a standard that was eliminated in the HIPAA Final Rule.

- Notification Recipients. HIPAA requires notification to HHS in addition to the individual and, in some cases, the media. Many states take a similar approach by requiring notification to the State Attorney General. Other states require notifying state law enforcement agencies or federal credit reporting agencies as well.

- Content of Notice. Although some states set forth specific requirements for the content of notification, many do not. The states that mandate certain content, however, have very different requirements, some of which conflict with each other.

- Industry Exemptions. Some state security breach laws exempt certain industries from notification requirements. Exempted industries are typically those in which other laws impose notification obligations, such as in the health care and financial industries.

2. State Laws Requiring Pre-Breach Safeguards

Like HIPAA, some states require entities that possess personal information to implement adequate security measures to prevent a breach of personal information.[72] Most states generically require "appropriate administrative, technical, and physical security safeguards" rather than providing the specificity in the HIPAA regulations. Typical provisions include:

---

[72] States with requirements for pre-breach safeguards include *inter alia* Arkansas, California, Indiana, Kansas, Montana, Nevada, New Jersey, North Carolina, Rhode Island, Texas, and Utah.

- Security Controls. Entities must use appropriate measures to protect personal information from unauthorized access, destruction, use, modification, or disclosure.

- Third-Party Contractual Restrictions. Entities must ensure that third parties vendors also implement reasonable and adequate security measures.

- Encryption. Although few states currently ***require*** encryption, this safeguard is increasingly gaining favor, particularly because most states do not require notification if the breached information was encrypted.

3. State Enforcement Actions Involving Breaches

State Attorneys General have increased enforcement of state laws involving security breaches. In most cases, the breached entity will enter into a settlement decree or "assurance of voluntary compliance" in which the breached entity does not admit wrongdoing, but still pays hefty fines and agrees to enhanced security measures. For example, after a security breach involving 5.9 million records stolen, Certegy Check Services, Inc. entered into an "Assurance of Voluntary Compliance" with the Florida Attorney General's Office requiring an enhanced security program and nearly $1 million in fines.[73]

State security breach laws add additional complexity and uncertainty to an already fragmented set of laws governing personal information. The presence of such laws means that an entity that possesses personal information and suffers a breach potentially faces a slew of investigations and enforcement actions from a wide variety of state and federal regulators, plus potential litigation from private plaintiffs.

D. Financial Information Security Standards

1. The Gramm-Leach-Bliley Act

The Gramm-Leach Bliley Act (GLBA) is designed to create minimum security standards for the protection of "consumers'" non-public personal information by regulating entities that provide financial services to individuals for personal, family, or household purposes. The GLBA's Privacy of Consumer Financial Information Rule ("Privacy Rule") applies to a broad range of "financial institutions," including many businesses not traditionally considered to be financial institutions, such as non-bank mortgage lenders, tax preparers, providers of real estate settlement services, and debt collectors.

---

[73] State of Florida Office of Attorney General, *In the Matter of Certegy Check Services, Inc.,* Case No. L07-3-1109 (Mar. 31, 2010) (http://myfloridalegal.com/webfiles.nsf/WF/MRAY-84KKQN/$file/CertegyAVC.pdf).

Attorneys and law firms engaged in the practice of law are not covered by the GLBA.[74] However, many attorneys have clients subject to the GLBA security rules. Furthermore, even if not applicable, the GLBA security requirements share many common elements with other security standards that law offices may find helpful in assessing their information security programs.

As described in more detail below, law firm clients that fall under the GLBA's reach are required to establish administrative, technical, and physical safeguards to protect consumers' non-public personal information (NPI). Law firms must be cognizant of their clients' obligations to protect consumers' NPI, and be sure that they too have adequate safeguards in place to protect client information. Moreover, clients may expect their law firms to follow security standards similar to those specified by GLBA.

a. General GLBA Security Requirements

The GLBA applies to businesses that are "significantly engaged" in "financial activities" as described in section 4(k) of the Bank Holding Company Act. A business's activities determine whether it is a "financial institution" under the Privacy Rule. If a business is subject to the GLBA, it must secure consumers' NPI that it holds.[75] "Consumers," in turn, are individuals who obtain, or who seek to obtain, financial products or services from a financial institution "to be used primarily for **personal, family, or household** purposes."[76]

Financial institutions subject to the GLBA must establish administrative, technical, and physical safeguards for the protection of consumers' NPI. Such NPI includes:

> personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution.

15 U.S.C. § 6809(4)(A). More specifically, financial institutions must:

(1) ensure the security and confidentiality of customer records and information;

(2) protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

---

[74] In *American Bar Ass'n v. FTC*, 430 F.3d 457 (D.C. Cir. 2005), the Court of Appeals for the District of Columbia Circuit struck down the Federal Trade Commission's attempt to regulate attorneys and law firms as "financial institutions" under the GLBA.

[75] 15 U.S.C. § 6801(a).

[76] 15 U.S.C. § 6809(9) (emphasis added).

15 U.S.C. § 6801(b)(1-3).

b. The Security Safeguards Rule

The GLBA gives authority to several federal agencies and the States to administer and enforce the security protections of the Act. The Federal Trade Commission (FTC) is the "catch-all" agency for GLBA enforcement (*i.e.*, the agency responsible for all entities not specifically regulated by another agency). The FTC has issued the "Security Safeguards Rule" which applies to the handling of customer information by those institutions that are subject to the FTC's jurisdiction.[77] The FTC has also published an extensive list of actions businesses can take to ensure they address three key areas of risk that the FTC has identified with respect to the required minimum security protections: employee management and training; information systems; and detecting and managing system failures.[78]

Companies subject to the Safeguards Rule must develop a written information security plan to protect customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. The basic elements of a security program require businesses to:

(1) Designate an employee to coordinate the information security program;

(2) Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling those risks;

(3) Design and implement a safeguards program, and regularly monitor and test it;

(4) Select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and

(5) Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

2. The Red Flags Rule

The FTC's Red Flags Rule,[79] promulgated pursuant to the Fair and Accurate Credit Transaction Act of 2003 (FACTA),[80] requires certain financial institutions and creditors to develop and implement a written identity

---

77 *See* 16 C.F.R. § 314.

78 This list can be found at: http://business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule.

79 16 C.F.R. § 681.1.

theft prevention program to detect, prevent, and mitigate identity theft. Prior to the Red Flags Program Clarification Act,[81] signed into law by President Obama on December 18, 2010, the Rule's definition of "creditor" was so broad as to encompass almost any business that allowed customers to defer payment until after the time of service, including law firms and medical practices. However, the Clarification Act narrowed the definition of "creditor" to include only businesses that regularly and in the ordinary course of business:

(1) Obtain or use consumer reports, directly or indirectly, in connection with a credit transaction;

(2) furnish information to consumer reporting agencies … in connection with a credit transaction; or

(3) advance funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person.[82]

The definition of creditor does not include businesses that advance funds on behalf of a person for "expenses incidental to a service provided by the creditor to that person."[83] Under this definition, law firms that accept deferred payment are not subject to the Red Flags Rule.[84] However, similar to the GLBA, many law firm clients are subject to the Red Flags Rule. Thus, law firms are well-advised to be familiar with their clients' obligations under the Red Flags Rule and know that clients may expect their law firms to handle their customers' information accordingly.

On June 12, 2013, the FTC issued guidance on how to comply with the Red Flags Rule. The guidance requires financial institutions and creditors to adopt the following basic elements of a security program:

(1) Identify relevant red flags, considering risk factors, sources, and categories of common red flags;

(2) Detect red flags, using for example identity verification and authentication methods;

(continued…)

80 15 U.S.C. § 1681m(e).

81 15 U.S.C. § 1681m(e)(4).

82 15 U.S.C. § 1681m(e)(4)(A)(i)-(iii).

83 15 U.S.C. § 1681m(e)(4)(B).

84 *See also Am. Bar Ass'n v. FTC*, 636 F.3d 641, 643 (D.C. Cir. 2011) ("The Clarification Act expressly amended the FACT Act, changed the definition of "creditor," and made it clear that a creditor's allowance of deferred payments alone could not trigger the identity theft protection requirements.").

(3) Prevent and mitigate identity theft by, among other things, being prepared to respond appropriately to red flags raised by the program; and

(4) Update the security program as a business changes, new red flags emerge, technology develops, and bad actors switch tactics.[85]

In administering a red flags program, businesses should monitor the activities of their service providers. One way to do that is to add a provision to contracts with service providers requiring them to have procedures in place to detect, report, and prevent or mitigate red flags. Lastly, the Rule requires that a company's Board of Directors, or an appropriate committee of the Board, approve the initial security program. The FTC guidance also advises reporting to the Board annually on the effectiveness of the program.

E. International Cybersecurity Standards

In addition to public sector standards, many organizations, and some law firms, are looking to the International Organization for Standardization standards as a blueprint for their information security programs, specifically ISO 27001, *Information Technology – Security Techniques – Information Security Management Systems – Requirements*.[86] This section will explore key elements of ISO 27001 certification emphasizing the same steps outlined in the section on NIST security controls: (1) establishing security objectives; (2) identifying security needs; (3) implementing a security program; and (4) ensuring compliance.

1. Establishing Security Objectives

ISO 27001 describes its purpose as providing a model and direction for defining, implementing, operating, monitoring, reviewing, and improving an Information Security Management System (ISMS). The ISMS itself is based on a business risk approach to maintain information security. ISO 27001 provides instructions for setting objectives that are appropriate, clear, and aligned with the company's strategic risk management.[87]

2. Identifying Security Needs

ISO 27001 prescribes a multi-step process for identifying security needs. Once objectives have been set, an organization must first identify its risks, taking into account its assets, the threats to those assets, and

---

[85] *See* FTC, Bureau of Consumer Protection, "Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business," http://business.ftc.gov/documents/bus23-fighting-identity-theft-red-flags-rule-how-guide-business.

[86] ISO / IEC 27001 (ISO 27001) was published in 2005 by the International Organization for Standardization and the International Electrotechnical commission. It is available in the United States through the American National Standards Institutes, ANSI, at http://webstore.ansi.org/RecordDetail.aspx?sku=ISO%2FIEC+27001%3A2005. ISO 27001 is only one part of a "Toolkit," that includes ISO 27001, ISO 27002, and more specific instructions for implementing a workable information security management system.

[87] ISO 27001 1.1.

vulnerabilities that might be exploited. Then the organization must assess the impact that the loss of confidentiality, integrity, or availability may have.[88]

Once an organization has identified these risks, the organization must evaluate the likelihood of security failures and analyze options to address those risks. Finally, the organization (or law firm) should select appropriate controls for the risks identified, and communicate the proposed controls to management.[89]

3. Implementing a Security Program

Once the risks have been identified and appropriate controls have been selected, the next step is to implement the ISMS. This includes formulating and implementing a risk treatment plan, as well as implementing the controls identified in earlier steps. It will also include implementing training and awareness programs for personnel and management regarding the ISMS. Perhaps most importantly, this step requires implementing a process to detect and respond to security events rapidly.[90]

4. Ensuring Compliance

ISO 27001 focuses on monitoring and improving security practices throughout the life of the ISMS. It prescribes a set of steps organizations should take to ensure compliance and improve their processes.[91] Among other things, organizations should:

- Execute monitoring and reviewing procedures. These procedures should be tailored to promptly detect errors in processing, quickly identify security breaches, allow management to determine the effectiveness of controls, and determine the effectiveness of reactions to security incidents.

- Review the effectiveness of the ISMS. Organizations should regularly review the ISMS, taking into account the security program objectives, whether the selected controls are appropriate or effective, and any feedback from the various stakeholders.

- Continually re-evaluate the risk. Organizations should review risk assessments at planned intervals and after any major organizational changes. These assessments should take into account changes to the threat, technology, and the regulatory environment.

---

88 ISO 27001 4.2.1

89 *Id*.

90 ISO 27001 4.2.2

91 ISO 27001 4.2.3

- Audit. Periodic audits of the program should address security breaches and responses, as well as risk evaluations, and should be presented to management.

- Strive for improvement. ISO 27001 directs organizations to seek to continually improve their processes. To that end, it directs organizations to regularly implement identified improvements in the ISMS, communicate these improvements to all stakeholders, and ensure that improvements are geared towards the stated objectives of the ISMS.[92]

5. Mapping To and From NIST SP 800-53

Companies (and law firms) that operate in both the public and private sectors might prefer a combined approach to security standards that incorporate both the ISO 27001 standards as well as the NIST 800-53 security controls. As one might expect, there is substantial overlap between the two. The recently-released and updated version of NIST SP 800-53 includes two tables for mapping ISO 27001 standards to the corresponding NIST SP 800-53 controls and vice versa.[93]

92 ISO 27001 4.2.4

93 NIST SP 800-53 Tables H1 & H2, Appendix H.