88-MAY N.Y. St. B.J. 38

New York State Bar Journal
May, 2016

DEFENSIBLE CYBERSECURITY

Tailoring an Organization's Security Posture to Applicable Legal Standards

Dino E. Medina [a1]

It's not surprising that security experts now regularly use phrases like "There are companies that have been hacked, companies that don't know they've been hacked, and companies that refuse to recognize they have been hacked." Although the storage of sensitive information in the digital space is the modern, convenient, cost-effective norm for law firms and the corporate entities they serve, the potential for misappropriation of this information is greater than ever. Over the past couple of years, data breaches stemming from both hackers and inadvertent disclosures have increased exponentially.

Everyone is talking about security, but how does such talk translate to a provable, defensible cybersecurity program? Law firm clients, corporate investors and regulators (collectively, stakeholders), now closely scrutinize the security measures of law firms and corporate entities, respectively, with the goal of creating greater accountability for the security of their sensitive electronic data. These organizations have responded by hiring outside consulting firms to build custom information security management systems.

What looks solid on the surface may sit on unstable ground. The creation of a typical information security management system entails conducting a risk assessment, creating security policies and testing the effectiveness of those policies. While a well-designed information security management system can provide a superficial level of assurance to stakeholders, the failure to place applicable legal standards for data security at the forefront of each stage of the program-building process is likely to result in ***39** the subject entity's inability to mitigate damages should an actual data breach occur.

John Verry, managing partner at Pivot Point Security, explains,

> It's hard to over-emphasize the value of strong risk assessment capabilities when building a comprehensive and provable information security program. It is only through the broader consideration of "nontraditional" information-related risks such as physical security, employees, contractual risk, laws/regulations, vendors and partners that an organization can protect itself from the diverse threats that are often the cause of today's largest breaches.

To better explore this issue, we set forth the elements used to assess an entity's security posture prior to the policy planning stage, offer a set of best practices to guide policy development, identify the types of accreditations available to such entities and illustrate how incorporation of applicable legal standards into each of these processes results in the most effective security risk mitigation system.

Key Risk Assessment Considerations

There are a number of formal data security **risk** assessment methodologies in existence, each with a different name applied to legitimize its application to a particular data type, industry, or set of activities. However, there are two elements that tie them all together - their purpose is to understand what **risks** exist to the entity applying them, and to document the likelihood and impact of each known **risk**. [1] The central question in any data security **risk** assessment is: Are the precautions an entity takes to secure its electronic data effective at controlling the types of **risks** the entity faces?

Identify Sensitive Data and Categorize It According to Applicable Legal Standard

The first step in the assessment process is to evaluate the sensitive data types the subject entity creates, collects, maintains or transmits, and categorize this data based on the legal framework governing its protection. **Law firms** and their corporate clients hold a variety of sensitive data types, each requiring a different standard for protection. Here are some examples of sensitive data types and the legal standard(s) applicable to the security of each.

The security of information an attorney learns during the representation of a client, including a corporate client, is governed by ethical standards for attorney conduct. For example, the American Bar Association's Model Rule 1.6(c) states "a lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to the representation of a client." [2] The comments to Rule 1.6 set forth factors that are to be used to determine the reasonableness of an attorney's efforts to secure his or her client's information. They include the below items. [3]

- Sensitivity of the information
- The likelihood of disclosure if additional safeguards are not employed
- The cost of employing additional safeguards
- The difficulty of implementing the safeguards
- The extent to which the safeguards negatively impact the lawyer's ability to represent clients generally

Personally Identifiable Information (PII) is any information about an individual maintained by an entity, including (1) any information that can be used to distinguish or trace an individual's identity (e.g., name, Social Security number, date of birth); and (2) any other information that is linked or linkable to an individual (e.g., medical, financial and employment information). Forty-seven states have implemented such laws and each requires appropriate administrative, technical and physical safeguards for PII.

Protected Health Information (PHI) is information traceable to a patient by one or more of 18 identifiers that relate to medical condition, diagnosis or treatment, [4] including:

- Name
- License number
- Dates (e.g., birth, admission, discharge, death)
- Vehicle identifiers
- Address
- Medical device identifiers
- Phone number
- Fax number
- URLs

- IP address
- Email address
- Biometric identifiers
- Facial photographs
- Social Security number
- Health plan number
- Medical record number
- Account number
- Any other unique identifier

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic PHI. The standard for satisfaction of the Security Rule is encryption of electronic PHI.

The security of intellectual property (IP) is typically governed by contract, applying a standard of care that the party receiving IP information uses to protect its own information of like importance. IP, whether in the form of patents, trademarks, copyrights or trade secrets, may be more valuable than an entity's physical assets. According to the Commission on the Theft of American Intellectual Property, U.S. companies lose hundreds of billions of dollars each year as a result of IP theft. [5]

***40** Once sensitive data and the legal standards applicable to their security are identified, it is time to understand and analyze the entity's security **risks**. For this step, it is necessary to examine all forms of **risk** that potentially impact security of sensitive data, including without limitation, regulatory **risk**, technical **risk** (i.e., gaps in the entity's physical and virtual security infrastructure), **risk** of human error (e.g., susceptibility to phishing, ran-somware or malware attacks), **risks** in physical security infrastructure (i.e., all points of entry into areas where sensitive data resides, including buildings, offices and server rooms), and **risks** in virtual security infrastructure (e.g., network access controls, software access controls, password protocols, and encryption of data in motion and data at rest [6]).

Assemble the Team

The next step in the assessment is to evaluate the entity's internal resources and assemble a team with the types of expertise necessary to thoroughly address the organization's **risk** posture. There are four categories of personnel required for this step:

- Legal personnel to advise with respect to the laws applicable to the data the entity holds;
- Technical personnel to advise with respect to software and infrastructure;
- Accounting personnel to advise with respect to the costs versus benefits of existing cyber-**risk** controls; and
- C-suite personnel for analysis of business processes applicable to sensitive data, whether there's existing organizational buy-in of **risk** mitigation strategies, and whether existing security controls are inhibiting the entity's growth progress.

The final component of the security assessment stage is to bring the entity's key teams together to link the business processes that access sensitive data, the people and technology used to support those processes, and the existing security

structure to evaluate areas of risk. This task requires the drafting of a risk assessment report in order to comprehensively address data security risks. Law firms and corporate entities should consider engaging an outside expert to assist in this task, as holes in risk assessment documentation will result in an ineffective cybersecurity program.

Drafting Effective Information Security Risk Management Policies

Once the law firm or corporate entity has assessed its data security risks using this framework, it needs to carefully craft information security management policies to control these risks.[7] To meaningfully address an organization's risk profile, the risk assessment report and legal standards governing security of the data must guide policy development. When drafting the policies, remember to include the following, often-overlooked, aspects:

- Closely link the legal standards governing security of the sensitive data to the policy requirements;
- Include verification of the entity's continuing compliance with the policies;
- Incorporate comprehensive employee training with periodic updates into the program, since studies have found that educating employees is vital to reducing data breaches;[8]
- Ensure third-party security risks are effectively managed;
  - Via contract, make certain they are legally bound to maintain data security in accordance with standards applicable to your sensitive data types, and
  - Stipulate audit requirements, recognizing the third-party vendors' confidentiality obligations to other clients.

Third-Party Verifications

If an entity's underlying information security methodology is properly designed and effectively implemented, external security verifications can both instill confidence in stakeholders and substantially mitigate damages in the event of a security breach. They can be used to test a law firm or corporate entity's own data security controls and those of its outside contractors. Various levels of external testing, audits and security accreditations are available, including the following - listed in order of testing rigor:

- SSAE-16 SOC 1 (Standard for security controls impacting financial reporting)
- SOC 2 (Standard for security, availability, processing integrity, confidentiality or privacy of information)
- ISO-27001: 2013 (International standard for information security)
- PCI DSS (Payment Card Industry standard for merchants)
- FedRAMP (U.S. Government standard for cloud services providers)

SSAE-16 SOC1 Type 2 Standard

The Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) published the Statement on Standards for Attestation Engagements (SSAE) No. 16 - Reporting on Controls at a Service Organization - in January 2010. The ASB defines a service organization as one that provides services to “user entities,” for which these services are likely to be relevant to the user entities' own internal controls for financial reporting.[9] The term “user entity” is simply an entity utilizing the services of a service organization.

The SSAE 16 standard requires a service organization to describe its "system" (i.e., the services the organization provides, along with the supporting processes, policies, procedures, personnel and operational undertakings that constitute the service organization's core activities relevant to user entities). In addition, **management** of the service organization must make a number of affirmative, ***41** written representations regarding its systems and the appropriateness of the design and operating efficacy of the organization's controls in satisfying their objectives [10] - for purposes of this article, the objective is information security, and the areas requiring **management** representations follow.

- **Management's** description of the service organization's "system" has to fairly and accurately represent the "system" as implemented throughout the time period subject to testing, which is typically six months.
- The control objectives referenced in **management's** description of the service organization's "system" have to have been appropriately designed to achieve those control objectives throughout the time period subject to testing; again, to be effective, the control objectives must closely track applicable legal standards.
- The controls have to have been consistently applied throughout the time period subject to testing.

An SSAE 16 information security audit and resulting report would include testing of the integrity, security and privacy of client data. Entities providing material outsourcing services to other entities (e.g., a **law firm** hosting client data for litigation purposes) would be well-advised to consider SSAE 16 third-party compliance examinations as a means of providing ongoing data privacy assurances to stakeholders and mitigating damages when a data breach occurs.

SOC 2 Standard

The AICPA Assurance Services Executive Committee released the current version of the Service Organization Control (SOC) 2 framework in January 2014. SOC 2 is a criteria-based framework that reports on a service organization's controls over one or more of the below Trust Services Principles (TSPs). [11]

- Security of a service organization's system (see SSAE 16 for "system" definition)
- Availability of a service organization's system
- Processing integrity of a service organization's system
- Confidentiality of the information that the service organization's system processes or maintains for user entities
- Privacy of personal information that the service organization collects, uses, retains, discloses and disposes of for user entities

An entity employing the SOC 2 framework may omit one or more of the five TSPs from the scope of its audit, provided each of the omitted TSPs is not applicable to the system under audit. [12]

Similar to an SSAE 16 information security audit, a SOC 2 audit would include testing of the subject entity's integrity, security and privacy of client data; however, there are two key differences: (1) as noted above, the SOC 2 TSPs include testing of additional system availability and information privacy controls; and (2) SOC 2 is tailored to technology and cloud computing service organizations, incorporating the TSPs in accordance with the Attestation Standards (AT) Section 101. **Law firms** and corporate entities storing client data in electronic form should consider SOC 2-based third-party compliance examinations as an alternative to SSAE 16 to bolster security and soften exposure should a data breach occur.

ISO-27001: 2013 Standard

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Joint Technical Committee published the ISO/IEC 27001:2013 information security standard in October 2013. It is a benchmarks-driven, internationally accepted specification for establishing, implementing, maintaining and continually improving an entity's information security management system (ISMS), covering both the entity's internal sensitive information as well as sensitive information entrusted to the entity by third parties. [13] The ISO/IEC 27001:2013 standard includes requirements for the assessment and treatment of an entity's information security risks that are custom-designed to address the entity's specific information security risk profile. Organizations meeting this security standard may gain an official certification issued by an independent and accredited certification body upon successful completion of a formal audit process.

ISO certifications are effective for three-year periods, provided the entity successfully completes interim annual spot inspections which demonstrate its ongoing compliance with the customized ISMS. More than the SSAE and SOC 2 attestations, the ISO/IEC 27001:2013 standard and its related benchmarks can act as guidelines for entities wishing to design defensible ***42** data security protocols. The benchmarks cover 14 domains:

- Information security policies tailored to legal/regulatory requirements
- Organization of information security
- Human Resources security (pre-employment, during employment and post-employment)
- Asset management
- Access control
- Cryptography
- Physical security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity
- Compliance with ISMS policies and applicable laws

PCI Standard

The Payment Card Industry (PCI) Security Standards Council launched the PCI Data Security Standard (DSS) in December 2004. The PCI DSS applies to any merchant, including any law firm or other corporate entity, which processes, stores or transmits credit card information. It requires a robust set of administrative, technical and physical security controls, including: [14]

- Install and maintain a firewall configuration to protect cardholder data
- Prohibit the use of vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks

- Protect all systems against malware, and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications
- Restrict access to cardholder data by business need-to-know
- Assign a unique user ID to each person with computer access
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security for all personnel

It is important to note that although all merchants that process, store or transmit cardholder data must implement and adhere to the PCI DSS, formal certification of PCI DSS compliance is not required for all merchants, particularly smaller ones. Nonetheless, to avoid liability for fraud associated with theft of cardholder data, **law firms** and other entities subject to PCI DSS are wise to undergo formal audits.

FedRAMP

Finally, the most comprehensive data security attestation is the Federal **Risk** and Authorization **Management** Program (FedRAMP). FedRAMP was implemented in December 2011 to provide assurances regarding the security of government data stored in cloud environments. It is a government-wide, standardized approach to security assessment, authorization and continuous monitoring for cloud-based products and services.[15] FedRAMP certification is a requirement for **law firms** and corporate entities seeking to host government data in a cloud-based (i.e., Internet-accessible) format.

The FedRAMP process incorporates the following five-step approach to certify a cloud-based service provider's (CSP) authorization to host government data:

1. Authorization Initiation: Federal agencies or CSPs initiate the FedRAMP process by pursuing a security authorization. There are two sub-steps to complete here.
   - Submit a formalized request for Authority to Operate (ATO) as a government CSP to the FedRAMP Joint Authorization Board (JAB);
   - Document and implement the required security controls and policies based on the level of **risk** posed by the types of government data at issue and the type of cloud system in which the CSP will store that data. Entities with other security accreditations (e.g., ISO/IEC 27001:2013) can leverage existing policies for this sub-step to save time, money and resources.
2. Security Assessment: The security assessment process must be conducted by an accredited third-party assessment organization (3PAO) and incorporates a set of baseline security controls for information technology systems developed by the National Institute of Standards and Testing (i.e., NIST SP 800-53 Rev. 3).
3. Review: 3PAOs send security assessment packages to the FedRAMP JAB for review.
4. Authorization: CSPs continue to work with federal executive departments and agencies to obtain ATO permissions.
5. Ongoing Compliance: Once an ATO is granted, ongoing security assessment and authorization activities must be satisfied to maintain the ATO.

The common link to all cyber security programs is their focus on the subject entity's operational controls within a risk framework that is acceptable to that entity.[16] The primary factors that influence an entity's acceptable levels of risk include:

- Legal requirements
- Client-specific requirements
- Amount of physical and monetary resources available for data security
- Types of data held
- Business sector in which the entity operates

Law firms and the corporate entities they serve act as vast repositories of both commercially sensitive information and ***43** PII, including PHI. The unauthorized disclosure of this kind of information could have a devastating effect on the responsible entity's reputation, financial position and, ultimately, the entity's ability to remain in business. Given the potential losses at stake when a data breach occurs, law firms and corporate entities must develop comprehensive cybersecurity programs, placing chief importance on the legal standards relevant to protecting their sensitive information.

Footnotes

a1 **DINO E. MEDINA** serves as general counsel at Complete Discovery Source, Inc. (CDS), a leading provider of electronic discovery services and a leading developer of data management solutions. In this capacity, Mr. Medina advises CDS on a variety of legal matters, including employment issues, contract drafting and negotiation strategies, dispute resolution, data privacy, security and compliance. Mr. Medina is a member of the New York Bar and the Electronic Discovery Committee of the New York State Bar Association. He teaches and speaks frequently on eDiscovery hot topics and best practices for deployment of legal technology. Mr. Medina lives on Long Island, New York with his wife and two children. This article is for informational purposes only and is not intended to constitute legal advice or to be relied upon.

1 https://www.optiv.com/blog/conducting-a-risk-assessment-key-com-ponents-you-cant-ignore.

2 http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/ru1e_1_6_confidentia1ity_of_information.

3 *Id.*

4 *See* 45 C.F.R. § 164.103.

5 http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf, p. 1.

6 Data in motion is data that is exiting an entity's network via email, the web or other Internet protocols, while data at rest is data in computer storage (e.g., data on a file server, hard drive or backup tape).

7 In addition to written policies, implementation of technical controls/standards/procedures (e.g., a state-of-the-art firewall, ant-virus software) is essential to a comprehensive cyber risk management program.

8 http://www.cio.com/article/2384855/compliance/most-data-breaches-caused-by-human-error--system-glitches.

9 http://www.ssae16.org/important-elements-ssae16/what-is-a-service-organization.

10 *Id.*

11 http://www.ssae16.org/white-papers/soc-2-reporting-framework-essentials-part-i.

12 *Id.*

13 http://www.iso.org/iso/catalogue_detail?csnumber-54534.

14 http://searchsecurity.techtarget.com/definition/PCI-DSS-12-requirements. Though framed as a legal standard herein, the PCI DSS is used by financial institutions as a formal **risk** assessment and compliance tool for merchants.

15 https://www.fedramp.gov/about-us/about/.

16 In the case of a FedRAMP-based **cybersecurity** program, acceptable **risk** levels are ultimately determined by the government agency engaging the CSP.