New Jersey Law Journal

Preventing a Data Breach: Considerations for Law Firm Security

Andrew Bolson, New Jersey Law Journal

October 30, 2014

The Gramm Leach Bliley Act regulates how businesses "significantly engaged" in financial activities protect consumer privacy. Financial institutions subject to the GLBA have certain regulatory obligations, including creating a written information security plan that considers a business' administrative, technical and physical security. The security plan is intended to consider the size and complexity of a business. Therefore, the security plan for a small accounting firm would not be expected to be the same as for a national bank.

In *New York State Bar Association v. FTC*, 276 F. Supp. 2d. 110 (DC Cir. 2004), attorneys and law firms were specifically exempted from the GLBA even if the law firm conducts financial services. According to the court, since lawyers were already required to maintain confidentiality and security protocols, it would have been nonsensical for Congress to pass redundant legislation and make lawyers subject to the GLBA. Despite not being regulated under the GLBA, all law firms should be creating security programs nevertheless. In fact, the American Bar Association recently passed a resolution encouraging law firms to implement cyber-security policies. Resolution 109 states:

Resolved, that the American Bar Association encourages all private and public sector organizations to develop, implement and maintain an appropriate cyber-security program that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected.

One of the reasons law firm cyber-security is becoming an increasing concern is because law firms are a prime target for criminal enterprises. Through a single law firm, criminals can gain access to client Social Security numbers, sensitive medical information and business trade secrets. In order to protect client information and uphold confidentiality requirements, law firms should be taking a cue from the GLBA and implementing policies regarding administrative, technical and physical security.

Administrative Security

A key aspect of administrative security is to develop and maintain data security policies and train employees on those policies on a regular basis. Policies should include protocols over password maintenance, file storage, document destruction and Internet and email usage. If law firms have policies but do not regularly train employees on how to implement them, the policies are useless. Periodic testing is one way to determine whether employees are abiding by security protocols. For example, if a law firm has a policy on not opening any suspicious email attachments, test emails can be sent to see whether employees follow the policy. Employees

who abide by the policy should be rewarded and employees who fail the test should be reminded of the policy's importance.

Vendor oversight is an often overlooked but essential component to administrative security. Any time client information is provided to a third party (i.e., documents sent to a copy vendor), the law firm loses control over how that information is secured. To ensure that the information provided to the third party will be protected, the law firm should be reviewing the vendor's security protocols, mandating that the vendor notify the law firm of any security breaches and require indemnification in the event of a breach, if possible.

Administrative security also includes protocols for dealing with terminated employees. When an employee leaves, whether voluntarily or involuntarily, the firm is particularly vulnerable. Upon leaving the firm, access rights to computer and email accounts must be terminated immediately. In addition, the firm should ensure that all laptops, smartphones or other storage devices in the possession of the terminated employee are timely returned.

Technical Security

Technical security covers computer network systems and access protocols. At the minimum, every law firm should be ensuring that antivirus security is up-to-date and that patches for security holes are continually uploaded. In addition, law firm administrators should be ensuring that employees maintain strong passwords that are regularly changed. Best practices for password include ensuring that passwords are not simple words that can be easily guessed but a combination of letters, numbers and symbols. Furthermore, administrators should ensure that login attempts are limited to prevent brute force attacks where hackers are able to attempt hundreds of thousands of password combinations until access is achieved.

A technical security policy must include provisions for copiers. Every modern copier contains a hard drive that stores an electronic version of all copies that have been made on the machine. Before a copier is trashed, sold or returned to a leasing agent, the hard-drive must be removed to ensure that the confidentiality of the data on the machine is not compromised.

Another component of technical security involves the transfer of data. In the event a law firm needs to share a client's financial information, trade secrets or other particularly sensitive information, law firms should be utilizing data encryption services. Data encryption is widely available and works by providing a key to the recipient of the information. Without the key to access the sensitive documents, the encrypted data cannot be opened by anyone but the recipient.

Physical Security

Physical security plans include analyzing the physical aspects of a law firm's office for potential security vulnerabilities. Planning for physical security should include ensuring that the doors of the office are locked when no one is working, that sensitive information, such as Social Security numbers, are filed away after use and that documents containing nonpublic personal information are shredded when disposed. A good practice for law firms is to provide shredders next to garbage cans or boxes next to garbage cans where attorneys can place documents to be shredded. These practices help to ensure that sensitive documents are not thrown into the garbage by mistake. If security practices, such as shredding, are consistently followed, the threat of data breach can be minimized.

While by no means an exhaustive list, the suggestions mentioned in this article are meant to

create a conversation within your law firm about data security. Simply, no law firm can turn a blind eye to this important issue because too much is at stake. As data breaches become more ubiquitous and the public becomes increasingly aware of data concerns, clients will be demanding and expecting that their law firm has the security infrastructure in place to keep their sensitive information secure. If a law firm does not meet their confidentiality obligation and suffers a data breach, the law firm may face reputational damage, ethics charges and even litigation. Implementing a data security policy that is geared to the particular size and nature of the firm may minimize the threat of a possible breach and the damage in the event that a breach does occur.
