October 2016
LEGAL MANAGEMENT
THE MAGAZINE OF THE ASSOCIATION OF LEGAL ADMINISTRATORS

Data Breaches: The Unavoidable Business Risk for Law Firms

Data breaches, like taxes, are inevitable. For law firms, cyber threats and data breaches are an inherent risk of doing business in the 21st century, and most still have significant work to do to protect themselves and their clients.

JAMES HARRISON
CEO
INVISUS

Firm administrators and executive management must be proactive in managing this unavoidable risk. Preventing data breaches and maintaining a formalized information security plan has become an essential business management practice for law firms, including yours. Here's why.

LAW FIRMS TARGETED

Increasingly, if a criminal wants information on a given company or organization, one of the first things they'll do is target the company's law firm. This shift was front and center in early 2016, when hackers targeted dozens of law firms working on M&A [mergers and acquisitions] deals.

Further evidence of this trend was noted in a 2015 technology and security survey done by the American Bar Association (ABA) that revealed up to 25 percent of firms have already experienced and reported a data breach. But because firms are usually hesitant to disclose breaches due to legal, ethical and reputation issues, industry experts say the percentage of breaches at law firms is likely even higher.

NEW AGE, NEW EXPECTATIONS

With the growing number of data breaches in the headlines, there is an urgency for firms to provide clients with assurances, if not evidence, that confidential client information is being properly secured.

Banks and other financial institutions typically require law firms to fill out up to 20-page questionnaires about their threat detection and network security systems. Health care industry clients are asking their law firms to do the same. Some clients are even sending their own security auditors into firms for interviews and inspections.

According to the ABA survey in 2015, 34 percent of firms have received security assessments from clients. Depending on the type of information the firm handles, these security assessment requests can follow one or more regulatory or industry security standards, including HIPAA, GLBA, SOC2, ISO 27001 or others. Your firm should be ready to respond to these types of security assessments and effectively demonstrate that you maintain a formalized information security plan that meets minimum standards.

In addition to ethical requirements, confidential and sensitive information must be properly protected under various federal and state regulatory requirements.

Firms that are serious about their business are making information security a priority, including obtaining security and compliance certifications based on regulatory and industry standards. Some firms are now starting to promote this type of certification in marketing materials and client pitches.

ETHICAL OBLIGATIONS

The ethical standards to ensure that attorneys and firms maintain client confidentiality are well known, as described in ABA Model Rule 1.6(c). Given the risks, it's reasonable that professional and ethical standards must now include the protection of confidential personal and business information against cyberattacks and data breaches.

In 2014, the ABA passed Resolution 109 encouraging all firms to "develop, implement and maintain an appropriate cybersecurity program … in accordance with accepted security frameworks and standards." In association with this resolution, the ABA Cybersecurity Legal Task Force reported that "first- and third-party losses associated with security incidents are rising, and cybersecurity is now one of the top risks organizations must manage."

REGULATORY REQUIREMENTS

In addition to ethical requirements, confidential and sensitive information must be properly protected under various federal and state regulatory requirements.

Well-known examples include HIPAA-HITECH for the health care industry and GLBA for the financial industry. These federal regulations include requirements that third-party service providers or "business associates," such as law firms, must safeguard confidential information in conformance with these federal data security and privacy regulations.

It's also important to note that 47 states have enacted statutes that protect the personally identifiable information (PII) of consumers and businesses within their state. Most state laws also include specific requirements for breach response, including reporting data breach incidents, notifying affected persons and victim remediation. Law firms located or who have clients in these states must comply with state laws or face civil and/or criminal penalties.

GETTING SERIOUS ABOUT SECURITY

Most law firms, large and small, do not have a formalized information security plan that encompasses all the necessary areas of risk and the related security controls. Each firm's situation is a little different, and each specific information security and risk management plan will be different.

The development, implementation and ongoing management of a firm's information security plan should follow the standards and best practices outlined in federal and state laws and industry platforms. Essential components to a successful overall information security plan include:

- Creating a culture of security, starting at the top
- Conducting regular risk and compliance assessments

- Maintaining updated security policies and procedures
- Implementing necessary cybersecurity technology and defenses
- Providing ongoing employee education and training
- Managing third-party supplier/vendor risks
- Having a breach incident response plan
- Reporting risks and results to executive management
- *Obtaining good cyber liability insurance*
- Getting third-party compliance certifications

The failure to implement and maintain one or more of these essentials can significantly reduce the firm's legal defensibility and argument that it had employed reasonable security measures.

MOVING FORWARD

The first step to protecting your clients and managing the risk of a data breach is to assess where your firm stands today. Where are your current vulnerabilities? What regulatory, legal and contractual requirements are you not adequately following, or failing to address altogether?

If you do not have the inside expertise in cybersecurity and compliance management — or if they are unwilling to make it a priority — get outside help. Take a comprehensive view of data breach prevention and compliance, and make sure you have the right people doing the right job for you right now.

ABOUT THE AUTHOR

James Harrison is the Founder and Chief Executive Officer of INVISUS. He is the market strategist and product visionary responsible for the development of the company's cybercrime, identity theft and data breach prevention and compliance product lineup. As an industry expert, Harrison regularly speaks and trains at various industry and trade conferences, including most recently at ALA's 2016 Annual Conference & Expo.

Email
LinkedIn
Phone: 801-724-6211