Law Firm Compliance Challenges Underscore Need for Renewed Cyber Security Focus

Today's regulatory environment can feel like a minefield. From SOX to HIPAA, GDPR to PCI DSS and new state privacy laws, complex regulations affect nearly every organization. And for attorneys, the landscape proves especially difficult. Each client potentially brings both sensitive data and additional regulations, adding to law firm compliance challenges.

Understand How and When Regulations Apply to Law Firms

Law firms occupy a unique position that makes them potentially subject to a wide range of regulations. Like any organization, they must comply with the evolving privacy laws of the state(s) in which they do businesses. However, in addition, they must take into account industry-specific data security and privacy laws that apply to any and all of their clients.

For instance, healthcare providers must adhere to the strict mandates of HIPAA, which requires them to safeguard protected health information (PHI). But HIPAA regulations also extend to "business associates" of those healthcare providers, who must also comply with HIPAA.

Therefore, any attorney who handles PHI must follow HIPAA standards. This includes attorneys dealing with cases involving personal injury, elder law, malpractice, and insurance defense. These firms need to implement the administrative, technical, and physical procedures to guard against inadvertent disclosure of PHI.

Additionally, law firms that take payment by credit card must comply with PCI DSS requirements. If they store personal data of European clients, they must abide by GDPR. If they deal with accounting and

investor data, they must follow SOX standards. And they should maintain a disaster preparedness plan in accordance with ISO and NIST recommendations.

Essential Compliance Responsibilities for Law Firms

The constantly evolving regulatory maze can prove complex. Fortunately, many of the regulations contain similar requirements. And, in any event, law firms have both an ethical and professional duty to protect client data and respond appropriately when breaches occur.

The American Bar Association (ABA) gives general guidance to law firms in ABA Rule 1.6. This rule indicates that attorneys should "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Additional ethics opinions provide more guidance on cyber security concerns.

In practical terms, these "reasonable efforts" will involve implementing the policies, procedures, and tools necessary to locate and secure sensitive information. They will also involve training staff to understand their roles relative to security and compliance. Further, firms must keep compliance in mind when entering into contracts with third-party vendors.

To prepare for the possibility of a breach, law firms should create and periodically update business continuity and incident response plans. And when breaches occur, they must be prepared to follow all reporting requirements.

Critical Consequences of Non-Compliance

While achieving and maintaining compliance can seem daunting, the risks of non-compliance are significant. For instance, HIPAA fines can skyrocket up to $50 thousand per violation for willful neglect

of rules, with a maximum fine of $1.5 million per year. But even if states attorney generals do not impose fines, non-compliance can have devastating effects.

Perhaps most importantly, non-compliance can destroy the firm's relationships with valued clients. It can result in malpractice consequences and damage the firm's reputation and ability to generate new business.

Best Practices to Address Law Firm Compliance Challenges

To avoid the consequences of non-compliance, law firms should implement cyber security and compliance best practices, including the following:

- **Provide compliance and security awareness training to all staff** – Through repeated, targeted training, ensure that all employees understand their compliance responsibilities. They should also know safe computing basics, including how to recognize phishing attempts.
- **Build information governance** – Know what data your firm holds or processes and where it lives. Tag sensitive data and implement proper data retention policies.
- **Implement basic cyber security** – At a minimum, this includes implementing encryption of sensitive data, as well as device-level encryption where appropriate. It also includes strengthening identity and access management, particularly for privileged users.
- **Conduct regular audits and continuous monitoring** – Regular compliance and security audits will highlight areas of vulnerability. In addition, data compliance monitoring will help ensure compliance and security controls prove effective.

Law firm compliance challenges and the consequences of failure to comply can seem daunting. But the IT consultants at Messaging Architects have the experience and tools necessary to assist law firms as they identify and implement compliance strategies.