Law Firm Cybersecurity Risk Checklist

The growing wave of cybercrime has targeted every company in business today, and law firms are no exception. However, law firms face a number of unique cybersecurity risks; securing a law firm is more important and more onerous than securing an organization of comparable size in another industry. Review the following checklist, and evaluate:

- What risk factors apply to your firm?
- What sensitive data must your firm protect?
- What professional obligations does your firm have?

Law Firm Risks Factors:

Technology Adoption: Law firms have been proactively adopting technologies to share legal data more efficiently and improve productivity. However, these solutions often expose firms to greater cybersecurity risks. *Does your firm have any of these risky technologies or policies?*

- **Work remotely.** When lawyers work remotely, they can access sensitive data from unsecured locations.
- **Bring your own device.** Personal devices operate outside of your organization's IT parameters and expose your firm.
- **Cloud-based office solutions.** Cloud office tools, such as Office365, Google apps, and Dropbox, streamline document management and sharing. However, these solutions increase the risk of exposing confidential legal data.

Cybersecurity threats: law firms are at risk for a wide range of cyberattack types, like all businesses. Furthermore, legal work and firm policies may put law firms at elevated risk for many attack types. Is your firm vulnerable to any of these attacks?

- **Phishing attacks:** targeted social engineering emails that steal credentials of high-ranking organization members. Legal partners are at high risk, because their credentials are so valuable to fraudsters.
- **Insider threats:** a malicious insider steals legal data for personal gain. Partners and associates have deep knowledge of which firm data is most valuable, and constitute a high risk insider threat.
- **DDoS attacks and hacktivism:** politically motivated actors attack an organization's systems, not for material gain, but to harm a perceived enemy. Because law firms often represent controversial figures, they are at high risk for these types of attack.
- **Ransomware attacks:** targeting employees that unknowingly download malware from malicious websites to encrypt all data on the machine.

Sensitive Data at Risk:

Law firm computer systems represent the densest concentration of high value confidential information in business systems today. Every line of practice represents a unique and tempting target for cybercriminals

Does your firm have sensitive data in the following practice areas?

- **Corporate clients** share material non-public information (MNPI) with law firms. In March 2016, the FBI warned law firms that criminal groups are known to be actively seeking cybercriminals to carry out MNPI theft attacks.
- **Trust and estate clients** share the personal information of high-net-worth individuals, including information that could be used to fraudulently access these clients' personal accounts.
- **Litigation teams retain information**—litigation strategies, significant evidence, smoking-gun documents, etc.—that can determine the outcome of pending lawsuits.

Obligation to Secure:

All businesses are bound by a number of industry-agnostic regulations to secure their sensitive data. However, law firms also have unique mandates and other pressures to secure.

- **ABA Resolution 109** specifies that "[c]ontinuous monitoring and log analysis are a critical part of an organization-wide risk management," a professional obligation for lawyers.
  Has your firm implemented continuous monitoring and log analysis?
- **Resolution 109** states that "To maintain a highly proactive security posture, potential threats must be investigated and targeted attacks detected in advance or addressed as they occur."
  Does your firm have dedicated staff prepared to detect and respond to threats as they occur?
- **Amendments to the ABA Model Rules of Professional Conduct** (Model Rules) adopted in 2012 explicitly state that "a lawyer's duty of competence includes keeping abreast of changes in . relevant technology." *Does your firm have the expertise to remain abreast of changes in cyber-threats and cybersecurity?*
- As a law firm, the most important data you hold is client information. Clients and prospective clients will each have their own cybersecurity requirements: a combination of regulations, professional mandates, and internal policy directives. *Can your firm provide and demonstrate the level of security your clients require, including meeting regulatory standards for their industries, such as HIPAA, SOX, and others?*

AWN CyberSOC Helps Law Firms Meet Security Requirements

- Managed detection and response meets ABA requirements
- Single pane of glass provides security across devices and systems
- Supports regulatory compliance exercises
- Identifies and remediates advanced, targeted, and persistent threats

ARCTIC WOLF

AICPA SOC

SOC2 Type II Certified

Contact us
arcticwolf.com
1.888.272.8429
info@arcticwolf.com