Law Firm Cybersecurity: A Checklist for Managed Detection and Response

Law Firm Data Breaches Are on the Rise:

22% of surveyed law firms suffered a security breach [1]

40% of assessed law firms were breached but did not even know it[2]

As data breaches make headlines with increasing frequency, protecting client data has become a top priority for the legal industry. Like all organizations today, law firms recognize the profound impact cybersecurity has on their business. That impact resonates throughout the field of law, in particular, since firms are often required to store and share vast amounts of data.

What makes cybersecurity a real challenge in the legal industry is that there are no clear-cut regulatory mandates. This makes things especially tricky when trying to devise sound strategies for dealing with today's pernicious threats. Unlike their clients in regulated industries that require mandatory compliance, law firms are left with little guidance on how to secure personal information and sensitive data. Without the right solution, firm and client data is increasingly at risk as cyber-threats continue to evolve.

Holding Law Firms Accountable for Cybersecurity

From client information to trade secrets, law firms have both ethical and legal obligations to protect their privileged data. For that reason, corporate counsels now place increasingly stringent cybersecurity requirements on their outside legal counsel.

Cybersecurity is now a significant problem for the legal industry. Law firms are being held to corporate clients' regulatory obligations, which can include FINRA, HIPAA, PCI DSS, and more. Recent breaches have raised third-party due diligence to top-of-mind consideration. This is especially true in the wake of high-profile breaches, such as what Target suffered as a result of a compromised HVAC vendor.

In effect, law firms frequently have the added complexity of focusing on client defense rather than simply their own cyber protection. And while due diligence as a part of vendor risk management is quite common, there is no agreed-upon framework or specific mandate for cybersecurity policies or procedures for law firms to follow to meet their clients' regulatory requirements.

[1] ABA 2017 Legal Technology Survey Report, https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security.html

[2] LOGICFORCE Law Firm Cybersecurity Scorecard Q1 2017

Key Steps to Follow

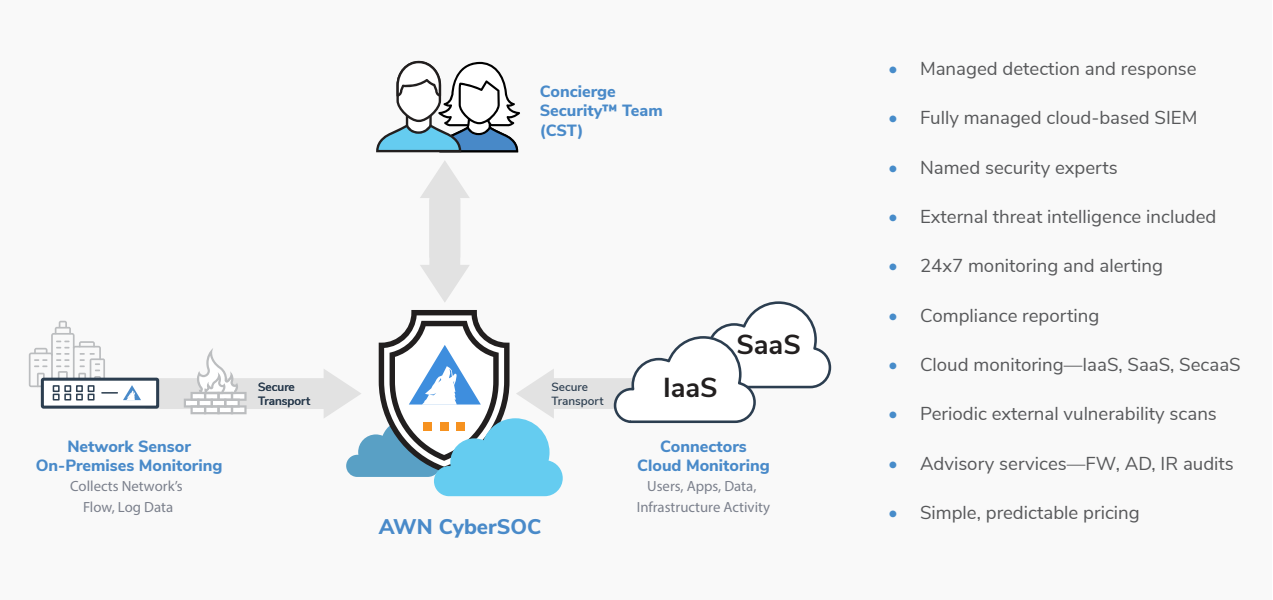
Despite the lack of cybersecurity guidance within the legal industry, corporate clients have continued to raise their level of expectations over time. So, to help law firms meet their clients' requirements, Arctic Wolf developed this checklist for managed detection and response (MDR)-based concepts provided in the ABA Cybersecurity Handbook. It provides direction on what you need to properly assess risk, monitor and detect threats to your network, develop plans for incident response, and create customized reporting for compliance and regulatory purposes.

Cybersecurity Requirement	Arctic Wolf's AWN CyberSOC™ Service
Risk Assessment	
Establish a risk profile	✓
Periodic security vulnerability assessment	✓
Monitoring, Detection of Unauthorized Activity & Response	
Continuous (24/7) network monitoring	✓
Subscription to threat intelligence (e.g. virus signatures, malicious IPs/domains, geo-location)	✓
Malware detection (e.g. ransomware, potentially unwanted programs)	✓
Cloud monitoring	✓
Network forensics analysis	✓
Detect unauthorized access and activity	✓
Manual and automated containment	✓
Incident Response	
Documented incident response review	✓
Named security team for triage and response	✓
Periodic live simulations to test IR protocols and teams	✓
Cybersecurity Governance	
Compliance reporting (example: PCI DSS, HIPAA)	✓
Workflow integration	✓

Arctic Wolf Monitors, Detects and Responds to Cyberthreats Against Law Firms

Your existing security controls can generate a lot of false positive alerts. If you're like most law firms, you don't have the time or resources to identify which ones matter and determine how best to respond to them.

The AWN CyberSOC™ service delivers customized security, while providing round-the-clock, on-demand access to a dedicated team of security experts—the Concierge Security™ team (CST)–who study a law firm's operating model and associated critical IT infrastructure to define what network segments, endpoints, and security devices to monitor. Arctic Wolf uses the most advanced, cloud-based SOC-as-a-service to ingest unlimited logs from your on-premises and cloud-based resources and apply real-time threat intelligence feeds to carefully evaluate indicators of compromise. This lets law firms realize the true value of outcome-based, customized security to identify incidents with utmost accuracy and minimize false positives.



Arctic Wolf's CST essentially become an extension to your IT and security teams. In general, the CST only engages customers when an incident requires immediate attention and provides detailed recommendations for actionable responses when specific steps must be taken. The CST knows that effective cybersecurity makes law firms like yours more prepared, more resilient, and better protected, so that you can continue to fulfill your obligations and best represent the needs of your clients.

ARCTIC WOLF

AICPA SOC

SOC2 Type II Certified

Contact us
arcticwolf.com
1.888.272.8429
info@arcticwolf.com