AGILEBLUE

Automation. Visibility. Confidence.

Legal Services

Whitepaper

AgileBlue, 2021

Overview

Law firms are prime targets of cybercriminals in today's hyperconnected world. As a result, law firms are expected to implement effective security controls around information relating to clients, investigators, and witnesses as part of their daily operation. This expectation applies to all law firms, regardless of their area of legal practice or size. It includes all aspects of how they store and handle highly confidential information, such as intellectual property, competitive company secrets, medical records, financial and payment data, or even sensitive government information.

Since law firms serve clients across multiple industries, they often must provide counsel on how to comply with industry regulations and cybersecurity requirements. For instance, healthcare clients may require cybersecurity measures related to the Health Insurance Portability and Accountability Act (HIPAA), and financial services firms may require compliance to the payment
card industry data security standard (PCI DSS). Large corporate customers also have their own security standards above and beyond industry requirements.

Meeting these diverse cybersecurity requirements is a challenge, and law firms unable to demonstrate the capabilities of a security operations center (SOC) will lose clients and fail to win new business. Cybercriminals are now capable of exploiting weaknesses at previously unseen speed and scale by rapidly acquiring new cyber weapons and continuously modifying their attack techniques. As threat actors continue to adapt and evolve, paying attention to cybersecurity strategy is paramount to law firms of all sizes.

At a Glance

- Cybercriminals target law firms of all sizes to monetize sensitive client data (ABA).
- Small & Mid-Size firms were victimized in 58% of breaches while 40% of the law firms breached didn't even know it (ABA).
- Prevention-focused cybersecurity solutions and point products consistently fail to deliver what they promise (PWC).
- Advanced threat detection SOC-as-a-Service is what law firms need to protect network infrastructure and client data.
- Law Firm of all sizes are being held to the various regulatory standards of their clients, including HIPPA, FINRA, SEC, GDPR, PCI DSS, GLBA/FFIEC, CCPA and more.

Cybersecurity Challenges in the Legal Industry

The legal industry has significantly benefited from digital transformation. Paper-based records and communications have long been replaced by email, video conferencing, connected databases, VoIP, cloud-based software-as-a-service (SaaS) solutions, and more. Unfortunately, these improvements in operational efficiency also come with increased risks. While law firms have been relatively quick to adopt and deploy promising technologies, they have yet to appropriately address the related security concerns.

The growing numbers of devices and applications at law firms today further exacerbates the problem:

Expanded attack surface: Every endpoint, network device, server, or application expands the attack surface, especially when attorneys or paralegals are required to access sensitive data remotely.

Hostile insiders: Weak or non-existent IT security standards for remote workers often lead to hostile rogue insiders jeopardizing the firm's business and its clients.

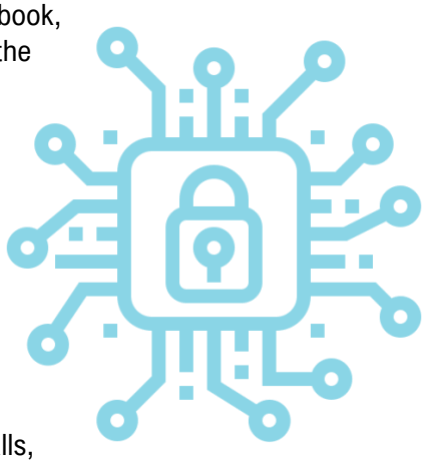
Human error: Lack of appropriate internal security training and poor supply chain risk management lets even well-intentioned employees or third-party vendors create accidental exposure

Firms without strong cybersecurity controls in place see diminished new business acquisitions and decreasing billables. The ability to adhere to compliance responsibilities is an important driver for new business. If a cyberattack compromises client data under compliance, law firms may also be subject to regulatory fines. With increasing guidance from U.S. government agencies such as the SEC and the FBI, as well as specific requirements from the American Bar Association (ABA), law firms now must prove the effectiveness of their cybersecurity strategies to constituents like auditors, board members, clients, and insurers. Per the ABA an increasingly high number of firms that are breached just don't know it. From a client's perspective, cyberattacks and breaches are the primary impetus behind technology audits, driving them to enforce even stricter security standards.

The Root Cause: IT Security Strategies That Have Consistently Failed

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a risk-based approach to managing cybersecurity risk. It defines a set of cybersecurity activities and desired outcomes. Unfortunately, implementing only a subset of the functions within the framework has proven to be insufficient. Most businesses still take 196 days to detect a security breach and another 77 days to contain it, while 40% of the law firms breached in 2016 didn't even know about it (Ponemon Research 2019).

While NIST provides a general framework applicable to all industries, the ABA has published a comprehensive guide specifically for law firms. The ABA Cybersecurity Handbook, created by the ABA Cybersecurity Legal Task Force, covers requirements in the following areas:

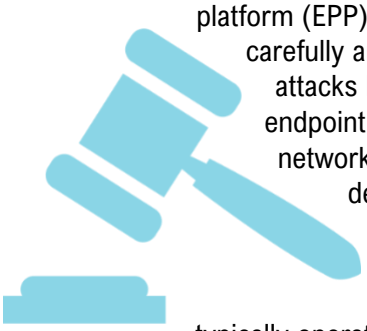


- Cybersecurity governance
- Risk assessment
- Protection of network and data
- Detection of unauthorized activity and response
- User training
- Risks associated with vendors and third parties

Law firms have attempted to meet elements of this guidance by deploying traditional endpoint antivirus (AV) solutions or perimeter defenses like firewalls, assuming these approaches will be enough to make their problems "go away." Unfortunately, these solutions have consistently failed to keep law firms secure. In some cases, law firms deploy security information and event management (SIEM) solutions. Unfortunately, SIEMs are extremely complex for firms to deploy, manage and operate. They, too, have failed to keep law firms secure.

Here are the top five types of cyberattacks that small and mid-size law firms tend to struggle with, and the reasons why traditional approaches have often failed (ABA 2019):

Ransomware is a type of malware that either threatens to block access to a victim's data, publish it, or destroy it unless a ransom in cryptocurrencies is paid. Firms may install AV or endpoint protection



platform (EPP) solutions on employee endpoints, but without having an expert team to carefully analyze their alerts and event log data, an attack can go unnoticed. These attacks have become particularly notorious for their ability to evade traditional endpoint controls, leaving most firms vulnerable as they operate without continuous network monitoring capabilities, real-time threat intelligence, or custom threat detection logic.

Phishing attacks seek to obtain sensitive information such as usernames, passwords, social security numbers or credit card numbers. Attackers typically operate under the guise of a trustworthy entity, such as a website for a bank, or the login page for an email or messaging service. Email security solutions that offer real-time analysis of URLs in emails, email attachments, and web objects can help with detection. But email security solutions are often unable to flag an embedded malicious URL or attachment before the victim interacts with it. In such cases, firms without continuous network monitoring, Active Directory (AD) monitoring, or advanced monitoring for any deployed SaaS applications are left vulnerable.

Adware and potentially unwanted programs (PUPs) are types of malware that an end-user likely never intended to install. PUPs typically display intrusive advertising and can track a user's Internet usage in order to sell information to advertisers. In-depth analysis of logs and alerts from AV solutions may help. However, attackers have rapidly modified their techniques. For example, runtime packers that decrease the size of executable files are widely used with PUPs, causing even known malware types to go undetected. Firms without continuous network monitoring capabilities to detect traffic from dangerous remote servers or scammer networks remain vulnerable.

Brute-force login attacks involve threat actors systematically attempting password or passphrase combinations until finding correct combinations and accessing restricted resources protected by the passwords. In-depth analysis of Active Directory logs and SaaS application login activity are the primary methods used to detect such attacks. Unfortunately, working with authentication data logs is complex and may require analyzing terabytes of data over a very short time period. Without access to the necessary expertise required to create custom detection logic, law firms may not even be aware of credential theft or ongoing data exfiltration.

Attacks on unpatched servers and infrastructure are specifically designed to exploit weaknesses and vulnerabilities in servers and other Internet-facing systems. In a vast majority of such attacks, patches are publicly announced and made available. For appropriate defense, law firms need access to advanced vulnerability scanning tools for system hardening and alerting. Ideally, they should also deploy continuous network monitoring tools with customized rules to detect anomalous scanning requests coming into Internet-facing entities, indicators of attackers probing the system.

NOTE

In each of these five attacks, simply installing AV or deploying basic perimeter defenses is no longer adequate. Industry experts now strongly advise law firms to reconsider their IT security strategies. Several recent attacks amplify this need.

A New Approach for a Secure Future: Adopting SOC-as-a-Service

IT teams at law firms only have a few hours to detect an intrusion, investigate the incident, estimate the severity and scope, determine what response actions are necessary, initiate the response, eject the attacker, and contain any damage. Given enough time, attackers can bury themselves deeper, start adapting their moves, and behave like an insider to make it look like whatever they're doing is just regular business activity. This makes detection at a later stage much harder and significantly impacts a firm's ability to trace their path during an investigation. This is exactly why law firms of all sizes need advanced threat detection and response capabilities with 24x7 security monitoring.

In the aftermath of most data breaches, IT teams find that attacks usually don't look like attacks at all, except in hindsight. Effective detection strategies depend on aggregating and correlating logs from critical components in an organization's network. Detecting patterns of anomalous activity and potential compromise requires the deep analysis of several critical log sources, including:

- Firewalls
- IDS/IPS
- Endpoint security (EPP, antivirus)
- Active Directory
- Email security gateways
- SaaS applications
- Cloud workloads

SOCs are staffed with trained security analysts who continuously monitor data centers and servers, user login activity, SaaS applications, cloud workloads, endpoints, and email systems. A SOC enables IT staff to correlate events across multiple, disparate systems, and extract actionable intelligence to aid effective threat detection and response. Unfortunately, its cost is well beyond the budget of most law firms. AgileBlue's SOC-as-a-service, CyberSOC, delivers the following capabilities at a simple and predictable monthly pricing model–essentially enabling smaller law firms to take advantage of security operations. Included are:

- Fully managed, cloud-based SIEM
- Machine Learning Engine
- External threat intelligence
- 24x7 monitoring and alerting
- Compliance reporting
- Cloud monitoring–AWS, Azure, Google Cloud
- Periodic external vulnerability scans

NOTE

Smaller law firms are increasingly targeted since they can be easy prey for cybercriminals seeking to infiltrate their much larger clients. Advanced detection and response is the last line of defense, and it's the difference between a threat compromising several attorneys' computers and the entire law firm's systems becoming infected.

Cybersecurity strategy is now a critical competitive differentiator for law firms of all sizes. Demonstrating strong cybersecurity controls is crucial to establishing and maintaining client confidence.

A SOC-as-a-service enables law firms to address the listed security gaps that result in the cyberattacks covered in the prior section going undetected. Using a managed SOC service gives firms complete centralized visibility into their networks' security and the ability to leverage existing point products and security investments. It also creates access to regular vulnerability assessments and enables firms to establish a detailed and customized incident response plan.

What's more, it helps law firms provide strong evidence of security processes during technology audits, avoid compliance penalties, and establish a new competitive differentiator, thereby increasing billables and accelerating new business acquisition.

The time for the legal industry to make strategic security improvements is now. Effective cybersecurity makes law firms more prepared, more resilient, and better protected so that they can continue to fulfill their obligations and represent the needs of their clients.

About AgileBlue

AgileBlue is a SOC-as-a-Service platform that's proven to detect cyber threats faster and more accurately across your entire digital infrastructure and cloud. We provide 24/7 monitoring, detection and response to identify cyber threats before a breach occurs.

Our tech is intelligent and automated, but we take a custom approach for every client we work with, analyzing and detecting exactly what you need it to. Our products are 100% cloud-based including advanced machine learning and user behavior analytics backed by our team of cyber experts who are always just a call away.

Ready to protect your company? Contact Us.