WHITEPAPER

PERSONAL | PREDICTABLE | PROTECTION

How Law Firms Can Protect Against the Top Five Cyberattacks

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 operations.

This expectation applies to all law firms, regardless of their area of legal practice. 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.

Despite recent innovative advances in security technology, many firms still struggle with common attacks that have been around for years, such as ransomware and phishing. This highlights the need for law firms to adopt a new approach to cybersecurity, one based on detection and response, and not just prevention.

This white paper is organized into three sections that address the most pressing cybersecurity challenges in the legal industry and explains:

- The current status quo in the legal industry and why cybersecurity should be top of mind for every law firm
- Why many existing IT security practices continue to fail
- Why customized detection and response is the most effective cybersecurity strategy for the legal industry

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

FAST FACTS

- Cybercriminals target law firms of all sizes to monetize sensitive client data
- Prevention-focused cybersecurity solutions and point products consistently fail to deliver what they promise
- Advanced threat detection and response is what law firms need to protect network infrastructure and client data

$1.5T

The underground cybercrime economy generates $1.5 trillion in annual profits

IBM Security, 2018

58%

The percentage of small businesses that were victimized of breaches[1] while 40% of the law firms breached didn't even know it[2]

[1] Verizon Data Breach Investigations Report 2018

[2] ABA Journal, March 2017

Cybersecurity Challenges in a Competitive 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.

Today's cybercriminals hold a strategic advantage, as they are able to launch attacks at a fraction of the cost—in terms of time, complexity, and resources—that law firms must typically spend to defend against them. This asymmetric nature of cybercrime is particularly pronounced in smaller firms that may lack financial resources or access to skilled security professionals. What's particularly alarming for the legal industry is that the global cybercrime economy generates an annual profit of $500 billion (from a total of $1.5 trillion) specifically from stealing intellectual property or trade secrets, facilitating through reinvestment their continued advances in attack techniques.

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.

Cyberattacks are non-discriminatory. Firms with just a few attorneys to those with thousands have all been targets. That's why all law firms need to ensure they have the appropriate security monitoring and threat detection capabilities in place before a client audit is performed. Firms can't afford to wait for external auditors to report a security issue that could have been internally discovered.

Most auditors will ask law firms if they have been breached in the last 60 days. Answering this question isn't always easy. Per the ABA, about one in four U.S. law firms with more than 100 attorneys self-reported having experienced a data breach in the last year. However, based on current research, 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.

FAST FACTS

- 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.
- The legal industry is subject to a code of conduct that requires law firms to appropriately allocate resources to manage risks and protect their clients' assets. Recent cyberattacks and data breaches have amplified the importance of third-party due diligence and, as a result, law firms of all sizes are being held to the various regulatory standards of their clients, including HIPAA, FINRA, SEC, GDPR, PCI DSS, GLBA/FFIEC and more. Technology audits are now an essential part of the process for law firms seeking to win and keep big clients.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

A common approach to IT security is to invest heavily in cybersecurity protection measures, or the "Protect" function in the NIST framework. Businesses typically deploy several perimeter and endpoint security products with the assumption that they are then secure.

The Root Cause: IT Security Strategies That Have Consistently Failed

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (Figure 1) is a risk-based approach to managing cybersecurity risk. It defines a set of cybersecurity activities and desired outcomes. The core of the framework consists of five concurrent and continuous functions: Identify, Protect, Detect, Respond, and Recover. A common approach to IT security is to invest heavily in cybersecurity protection measures, or the "Protect" function in the NIST framework. Businesses typically deploy several perimeter and endpoint security products with the assumption that they are then secure.

Unfortunately, implementing only a subset of the functions within the framework has proven to be insufficient. Most businesses still take 214 days to detect a security breach and another 77 days to contain it[1], while 40% of the law firms breached in 2016 didn't even know about it.

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

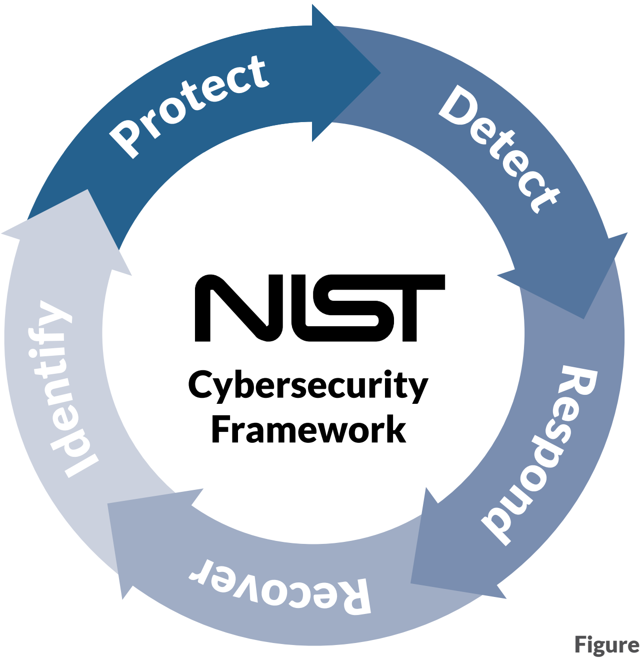


Figure 1

Law firms have attempted to meet elements of this guidance by deploying traditional endpoint antivirus (AV) solutions or perimeter defenses like firewalls (FWs), assuming that 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.

[1] Ponemon Institute's Global 2017 Cost of a Data Breach Study

FAST FACTS

- Law firms engaged in activities like eDiscovery are required to handle sensitive third-party data, including IP such as source code, and manage it though the lifecycle of the eDiscovery process. For such firms, displaying a strong cybersecurity posture gives them a distinct competitive edge.
- The ABA Cybersecurity Handbook outlines the key legal requirements, ethical issues, and special considerations for lawyers and practitioners of all types. The ABA requires law firms to establish a variety of cybersecurity procedures, including those relating to detection, response, and remediation. They include identifying likely attack vectors, identifying internal and external threat actors, and implementing a very detailed set of measures for detecting unauthorized activity and incident response.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

Based on Arctic Wolf™ data, here are the top five types of cyberattacks that smaller enterprises tend to struggle with, and the reasons why traditional approaches have often failed.

- **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 in to Internet-facing entities, indicators of attackers probing the system.

In each of the above 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.

FAST FACT

- Most law firms have traditionally adopted IT security strategies without the necessary controls to meet the ABA's guidance for detection and response, which includes continuous monitoring, aggregation/correlation of logs from multiple sources, forensics for determining the scope of a breach, and procedures for remediation. Law firms continue to only invest in prevention-based security products such as endpoint AV solutions and strategies based on deploying in-house SIEMs that have consistently failed to deliver on their promise to keep law firms secure.

IN THE NEWS

DLA Piper: *On the morning of June 27th, 2017, those entering the DC offices of DLA Piper were greeted by a whiteboard in the lobby with the following message, "Attention: DLA Employees. All network services are down, DO NOT turn on your computers! Please remove all laptops from docking stations & keep turned off. No exceptions." Emergency text messages were sent to the rest of the firm's employees with the same warning. The phone systems, email, and the law firm's web portal were all down.*

Operations ground to a halt, with all 4000 attorneys and support staff distributed across 40 countries unable to communicate or access any documentation. DLA Piper had been infected by the Petya malware, a strain specifically designed for data destruction. It took the firm several weeks to fully recover, and estimated costs from the attack are in the millions of dollars.

With the attack landscape rapidly evolving, law firms have an ethical and, more definitively, a regulatory obligation to secure their operations and disclose any breach. Cybersecurity has a significant reputational impact that requires redefining the security mindsets for partners, associates, and paralegals.

With the attack landscape rapidly evolving, law firms have an ethical and, more definitively, a regulatory obligation to secure their operations and disclose any breach. Cybersecurity has a significant reputational impact that requires redefining the security mindsets for partners, associates, and paralegals. For example, at firms dealing with a variety of clients, a common question might be, "If the medical malpractices partner clicked on a malicious URL, do we have to tell all our mergers and acquisitions clients that they're at risk?"

Unfortunately, the answer to this question can be extremely complex. It depends on the type of device the victim used; details on the specific website or email the link came from; the system state of the specific application the partner was running; the nature of the potentially malicious download; whether the malware was detected at the application, the endpoint, or in the network; how quickly the incident response processes were able to contain the threat; and whether the malware infected other systems on the network (moved laterally). Only once all these factors are accounted for is it possible to determine the true extent of the damage. Simply investing in prevention tools such as endpoint and perimeter solutions doesn't let a firm answer such a question. Furthermore, this is just one vector mapped to the malware attack. What about phishing, brute-force logins, and all the other attacks?

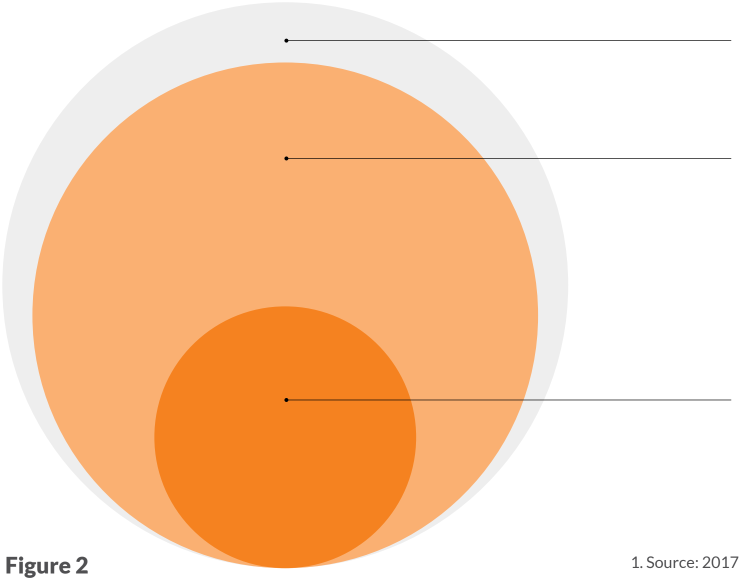
FAST FACT

▶ 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.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

Why Focus on Detection and Response?

Lower Your Cost of Handling Security Breaches by Speeding Up the Time to Identify and Contain the Attack



365 Days

291 Days

The lifecycle of a breach caused by a malicious attack. The Mean Time to Identify (MTTI) the breach for most businesses is **214 days**.

77 Days

The MeanTime to Contain (MTTC) the breach for most businesses.

Figure 2

1. Source: 2017 Ponemon Cost of Data Breach Incident Report

A New Approach for a Secure Future: Adopting Managed Detection and Response

In 2017, businesses took 214 days on average to identify malicious and criminal cyberattacks and 77 more days to contain the threat (Figure 2). What's more, it currently takes attackers only a few hours to move laterally from the initial Internet-facing server, endpoint, or other initially compromised system (the beachhead) to other machines within the network.

IT teams at law firms, therefore, 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

Large enterprises are able to achieve such advanced levels of security by building and staffing up a 24x7 security operations center (SOC). 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.

FAST FACT

- While the current version of the LSAT is administered to law school candidates for 3 hours and 30 minutes, it takes today's cybercriminals half that time to move laterally across a network to a system that may hold sensitive data.

©2020 Arctic Wolf Networks, Inc. All rights reserved. | Public

Complicating matters, the cybersecurity skill shortage is a recognized problem across industries. Not only do law firms need the budget to procure the necessary technology to build a SOC, they also have to hire experts with the specialized skills necessary to operate it. The skills gap–the disparity between what organizations need and the personnel they have the budget to hire–leaves law firms vulnerable. For most, hiring an in-house security operations team simply isn't feasible. Instead, they rely on ineffective consumer-grade security solutions, install several point products, or bury themselves in alerts from a SIEM they aren't able to manage.

Fortunately, with managed detection and response (MDR), the balance of power is slowly shifting away from cybercriminals and back to small businesses.

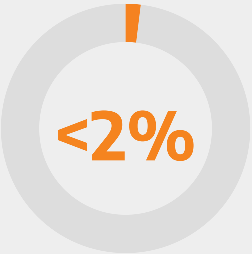
The Arctic Wolf SOC-as-a-service with Arctic Wolf™ Managed Detection and Response delivers the following capabilities at a simple and predictable pricing model–essentially enabling smaller law firms to take advantage of security operations equivalent to that of a Fortune 100 enterprise. Included are:

- ▶ Fully managed, cloud-based SIEM
- ▶ Human-assisted machine learning
- ▶ External threat intelligence
- ▶ 24x7 monitoring and alerting
- ▶ Compliance reporting
- ▶ Cloud monitoring–IaaS, SaaS, SecaaS
- ▶ Periodic external vulnerability scans
- ▶ Advisory services–FW, AD, IR audits

The Arctic Wolf SOC-as-a-service delivers customized security, while providing round-the-clock, on-demand access to a dedicated team of security experts. This team studies a law firm's operating model and IT posture to create custom threat detection logic suited to a firm's security needs and uses the most advanced technologies and real-time threat intelligence feeds to carefully evaluate indicators of compromise. This lets law firms realize the true value of outcome-based, customized security with fewer alerts and minimal false positives. In fact, the dedicated security experts become trusted advisors, extending customer IT and security teams, as they perform threat detection, triaging, and forensics. They typically only engage customers when an incident requires immediate attention, and provide detailed recommendations for actionable responses when specific steps must be taken.

A SOC-as-a-service enables law firms to address the security gaps that result in cyberattacks—such as those 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.



The percentage that law firms invest of their annual revenue on securing client data. Moreover, most of this investment goes to procuring outdated, ineffective solutions. In too many cases, firms risk having a breach.

The total annual revenue of U.S. legal services forecasted approximately $288 billion in 2018.

Chase Cost Management report

About Arctic Wolf

Arctic Wolf Networks delivers personal, predictable protection from cybersecurity threats through an industry-leading security operations center (SOC)-as-a-service. Arctic Wolf™ Managed Detection and Response and Managed Risk services are anchored by the Arctic Wolf Concierge Security™ Team who provide custom threat hunting, alerting, and reporting. The Arctic Wolf purpose-built, cloud-based SOC-as-a-service offers 24x7 monitoring, risk management, threat detection, and response. For more information about Arctic Wolf, visit arcticwolf.com.

©2020 Arctic Wolf Networks, Inc. All rights reserved. Arctic Wolf Networks, AWN and the Arctic Wolf Networks logo are trademarks of Arctic Wolf Networks, Inc. in the United States and/or other jurisdictions. Other names used in this document are for identification purposes only and may be trademarks of their respective owners.

SOC2 Type II Certified

Contact Us

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com