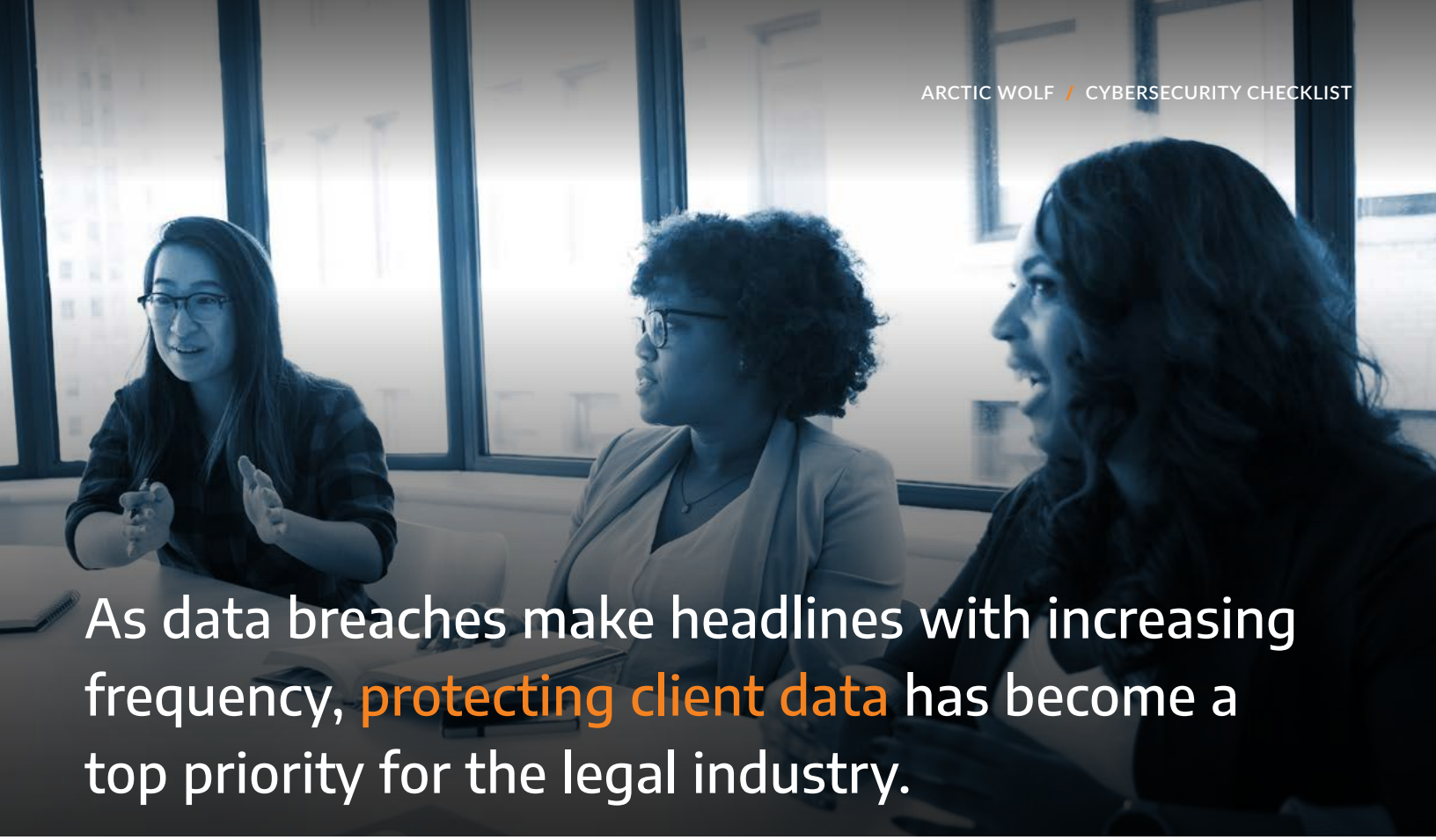
ARCTIC WOLF

The Legal Cybersecurity Checklist



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 private data. Because of this, law firms find themselves as prime targets for cyberattacks.

Making cybersecurity an even greater challenge for the legal industry is that instead of a single overarching mandate to follow, they must comply with a number of sweeping regulations—or risk facing harsh financial penalties.

With these factors in place, it can be tricky to devise sound strategies to deal with today's threats. That's why we've developed this Legal Cybersecurity Checklist.

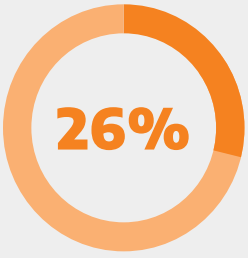
Now learn how to build a stronger security posture with advice, tips, and instructions on how to best secure your firm's data.

Since 2011, 80 of the top 100 law firms have suffered a data breach.[1]

Create a Security-Conscious Workforce

Without proper security awareness, people often use shortcuts to try and work more efficiently. Along the way, however, they sometimes engage in sloppy practices—like keeping passwords on a sticky note stuck to their monitor.

Creating a security mindset and culture at your law firm is the best way to mitigate the risks of human error.



Percentage of law firms that reported experiencing some sort of security breach in 2019.[2]

- **Implement an ongoing schedule of training and education.** Security should be a top concern for all individuals across an entire organization. From secretaries to paralegals to lawyers, everyone should be aware of security risks and what can happen in the event of a breach. Make sure to include updates on known attacks and provide information on best-in-class security procedures, such as two-factor authentication and password managers.
- **Monitor IT processes for complexity.** Keep ease of use in mind whenever you update or alter processes to avoid having users turn to insecure shortcuts.
- **Restrict access to data and applications.** Only give information access to individuals who need it to perform a particular job. Make sure this same protocol is implemented for physical access.
- **Implement data usage controls.** Block unsafe actions like uploading data to the web, sending emails to unauthorized addresses, or copying to external drives.
- **Establish a password policy.** Require regular password changes. In addition, make sure passwords are strong and not written down anywhere. This is an easy way to secure your data. Don't put your firm's reputation at risk by potentially exposing client information.

Inventory and Control: Hardware and Software Assets

You can't secure assets you don't know you have.

Reducing your firm's attack surface starts by having a complete view of all devices on your network. Keep track of every device at your firm and make sure to continually update this list whenever something new is added.

Once all your assets are audited, set up a disciplined schedule of updating, retiring, and protecting these assets. This helps deny hackers the opportunity to strike.

Without these practices established, there are far too many opportunities to access a firm's networks via unpatched devices—allowing hackers to steal records from internal systems.

- **Document and secure all devices that could access the network.** This includes laptops, cell phones, onsite hardware, and staff personal devices. Use inventory tools to keep up-to-date records of existing software and hardware.
- **Establish guest networks for the firms' offices and ensure that staff and visitors use the correct networks.** Find any slowdown spots or dead zones on the property. Keep clients and visitors on their own network and away from anything where they could access private information.
- **Oversee all user access to the network.** Record authentication errors and unauthorized access, and sweep the network for unusual activity. Also make sure to quickly disconnect any unauthorized devices you detect from the network, as well as any devices that run potentially dangerous software.

Continuously Analyze, Prioritize, and Manage Vulnerabilities

Legal IT teams must have 24x7 real-time cybersecurity operations that can manage vulnerabilities, monitor and detect threats, and respond to malicious and risky activity in real time. Otherwise, firms leave themselves open to major compliance risks. So, assess your risks and be proactive.

- **Continuously analyze.** Without the implementation of 24x7 monitoring coverage and continual analysis of possible threats, firms leave themselves open to a potential attack. According to the 2017 ABA legal Survey, 22% of firms were hacked or experienced a data breach in 2017. This marked a 14% increase from the year before.
- **Identify vulnerabilities and prioritize** what needs patching. A risk-based approach to vulnerability management enables an organization to eliminate vulnerabilities in a methodical fashion, starting with the most severe risks before addressing less severe ones.
- **Manage compliance risks.** Hefty fines and penalties are a major risk for law firms across the country. Opinion 483 lays out a lawyer's obligation after a data breach or cyberattack. Lawyers must keep clients "reasonably informed" about the status of a matter, and explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation."

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Manufacturers design default configurations with user experience and ease of use in mind. Basic controls, legacy systems, old protocols, preinstallation of unneeded bloatware, and open ports are easy targets for cybercriminals.

Good configuration doesn't stop when users get access to devices, as you'll need to watch continuously for changes when systems are patched or updated.

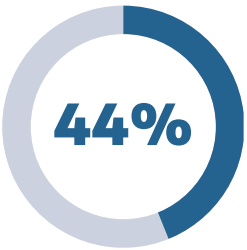
- **Train staff on anti-virus and anti-malware requirements** and the process for implementing automatic software updates to ensure that vulnerabilities are patched safely.
- **Configure items before they're put into use** and remove default settings and passwords.
- **Evaluate and enforce** software updates and security patches.

Maintain, Monitor, and Analyze Audit Logs

Without audit logs, attacks may go unnoticed and uninvestigated. That leaves the door open to additional attacks and untold potential damages. Most IT teams keep audit records for compliance purposes, but log data can also serve as proof in the event of a data breach that personal data didn't fall into the hands of a cybercriminal.

When law firms keep detailed log data, they can know if and when a cyber incident requires notifying customers or regulators, as well as avoid the potential fallout that occurs when the size and scope of a breach is unknown.

- **Log, monitor, and analyze security risks**. Without audit trails, law firms are forced to leverage complex (and costly) forensics practices to determine the severity of security incidents. Logging data can also satisfy regulatory requirements and help firms avoid further scrutiny.
- **Perform regular risk assessments** to identify weak points in your networks.
- **Be ready to report.** Use managed vulnerability assessment services to gain an understanding of your organization's IT security posture and risk profile.



Percentage of law firms that reported using file encryption in 2019, while even fewer used email encryption.[3]

Back up Data Offsite

In ransomware attacks, cybercriminals who steal data or hold systems hostage will only return it upon payment of a ransom. A second cache of critical data is essential to avoid having to pay a ransom. It also enables data recovery in the event of a natural disaster or system failure. With backed-up data, you can get up and running with uninfected copy, allowing you to minimize downtime.

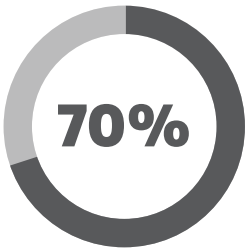
- **Maintain a current, flexible, secure, and speedy process to access data at all times.** Organizations need a recovery solution that allows them to recover data and bring applications back online as seamlessly as possible.
- **Consider cloud and physical backup solutions** and develop a backup schedule that takes the frequency of data changes into account.

Develop a Detailed Response Plan

Notifying customers and regulators of a breach is a costly process. Even if your firm isn't ultimately held liable, the damage to your reputation and countless hours spent attempting to rectify the situation can spell disaster for firms of every size.

Having a plan to not only prevent breaches, but also respond to cyber incidents in real time, is critical.

- **Ensure that data protection tools and policies are implemented and followed** so you can demonstrate compliance with regulations when audited.
- **Hire a data protection officer and establish written contracts with external partners** to ensure compliance across the firm.
- **Record all data breaches** so you can, when necessary, report them to relevant authorities. Or look to integrate with a partner who will document and report on vulnerabilities and breaches.



Percentage of law firms that report their clients have placed pressure on them to increase internal data security.[4]

Know Your Compliance Risk

In addition to federal and international data privacy regulations (including HIPPA, DCI, and GDPR), state legislatures have passed increasingly stringent requirements when data is accessed without consumers' express permission. All 50 states have some form of notification requirement when a breach occurs, timelines to notify, and obligations to provide complimentary credit monitoring; and the expanding definition of "personal information" will make compliance increasingly complicated for law firms.

Recent notification requirement expansions among states include; Massachusetts, Virginia, Texas, Washington and New York.

Massachusetts

(HB 4390)– Massachusetts expands data breach notification obligations

Amendments to the Massachusetts' data breach notification law went into effect on April 11, 2019. The amendments require businesses to offer complimentary credit monitoring for 18 months if a breach involves a resident's Social Security number. Furthermore, they must provide breach notifications on a rolling basis to avoid delay; and, if the exposed data is owned by a third party, then the notice must identify that third party. Lastly, businesses must inform state regulators as to whether they maintain "a written information security program."

Virginia

§ 18.2-186.6. Breach of personal information notification

This Code of Virginia defines a breach as "the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth."

Texas

(HB 4390) – Texas adds definitive notification timeline and establishes an advisory council

Effective January 1, 2020, amendments to the Texas Identity Theft Enforcement and Protection Act law require businesses to send breach notifications (1) to affected individuals without "unreasonable delay," but no later than 60 days after identifying such breach, and (2) to the Texas Attorney General within 60 days of identifying the breach, provided that the breach affects at least 250 Texas residents. Moreover, the law establishes a Texas Privacy Protection Advisory Council consisting of 15 appointed members who are "to study data privacy laws in [the] state, other states, and relevant foreign jurisdictions."

Washington

(HB 1071)

Effective March 1, 2020, the definition of "personal information" is expanded to include the following categories: birthdate; unique private keys for signing electronic records; student, military, or password identification numbers; medical information; biometric information; and online login credentials. Businesses may send breach notifications by email, unless the breach involves the credentials associated with that email account. If the breach affects more than 500 residents, then the entity must provide notice to the Attorney General, identifying the type of information exposed, the time frame of exposure, the steps taken to fix the breach, and a copy of the notice sent to affected individuals. Entities must provide updated notice to the Attorney General if any information required to be provided to the Attorney General is unknown at the time the notice is filed. Lastly, the law reduces the prior 45-day notification timeline to 30 days.

New York

(Senate Bill S5575B)

This bill relates to notification of a security breach, includes credit and debit cards, and increases civil penalties. Effective July 25, 2019, New York's breach notification law was amended to expand the definition of a "breach of the security of the system" and "private information," along with enacting a "reasonable security requirement" for New York's general business law, among other additions.

The Next Step in Legal Cybersecurity

When it comes to keeping your firm safe, you need experts in your corner. Arctic Wolf® delivers 24x7 security from experienced Concierge Security® Teams who face the gamut of cyberthreats every day.

Discover how Arctic Wolf's SOC-as-a-service helps law firms improve their security posture and check off the items on your security list in the most comprehensive, secure, and affordable way possible. Contact us today to schedule a demo.

EXPERIENCE ARCTIC WOLF'S INDUSTRY-LEADING CYBERSECURITY AT YOUR LAW FIRM

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf™ Platform, we provide security operations as a concierge service. Highly trained Concierge Security® experts work as an extension of your team to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture.

For more information about Arctic Wolf, visit arcticwolf.com.

1. https://news.bloomberglaw.com/business-and-practice/wake-up-call-80-of-100-big-law-firms-have-been-hacked-since-2011
2. https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/cybersecurity2019/
3. https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/cybersecurity2019/
4. Cyber Security and Law Firms: Defeating Hackers, Winning Clients from ALM Intelligence

ARCTIC WOLF

SOC2 Type II Certified

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

Contact Us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com