Protexure
(One of The McGowan Companies)

Create a Cybersecurity Policy for Your Law Firm

Cybersecurity threats facing law firms are becoming increasingly perilous, and data breaches are escalating yearly. In 2024 alone, at least 21 law firms reported breaches to their state attorney general in the first five months of the year, a stark reminder of the cyber vulnerabilities plaguing the legal industry.[1] For context, only 28 breaches were reported in 2023, highlighting a concerning upward trend that suggests a growing crisis.[1] The American Bar Association (ABA) estimates that nearly 30% of all law firms experienced breaches in 2023[2], indicating that the number of incidents may be significantly higher when considering unreported or unnoticed cases. The rise in class action lawsuits exacerbates this issue, with over 40 cases filed monthly against organizations that fail to protect sensitive client data.[1]

Many attorneys are acutely aware of the consequences of cyberattacks, including severe regulatory fines, costly litigation, and irreparable reputational damage. However, for small firms and solo practitioners, the burdens of cybersecurity can be overwhelming. Adding cybersecurity to the myriad responsibilities already top-of-mind can feel daunting. Yet, the ABA has clarified that safeguarding client information is not just advisable but obligatory; lawyers must take every reasonable step to protect their clients' sensitive data.[3]

This e-book serves as an introductory guide for legal professionals seeking to navigate the complexities of cybersecurity. By equipping yourself with the knowledge to bolster your firm's cyber defenses, you not only protect your clients but also enhance the integrity and trustworthiness of your practice in an increasingly digital world. Embracing these measures is not just a matter of compliance; it's essential for thriving in today's evolving legal landscape.

Conduct a Risk Assessment

Just how vulnerable is your firm to cyberattacks? Conducting a thorough data audit and risk assessment is your first line of defense. This proactive step allows you to map the flow of sensitive information while exposing the most significant vulnerabilities that bad actors could exploit.

A comprehensive data audit offers many insights into crucial aspects of your firm's data practices. You will better understand what sensitive data is collected, its storage and protection mechanisms, and who has access to it. Even more critical is your awareness of the data shared with third-party vendors: understanding what information they hold, how they utilize it, and most importantly, the safeguards they have in place to protect that data.

Engaging with an external cybersecurity firm is highly recommended for a robust evaluation, yet an independent data audit can also be immensely valuable. Start by crafting a list of targeted questions designed to uncover the intricacies of your data handling processes:

- How is sensitive data collected, and are the methods employed compliant with privacy standards?
- What protocols govern the storage of sensitive data, and how resilient are they against unauthorized access?
- What specific encryption measures are in place to protect data at rest and in transit?
- Who has access to sensitive data, and is their access level justified?
- Where are the potential weaknesses in your cybersecurity framework that could leave your firm vulnerable?
- Are all my passwords secure, and are they managed following best practices? What methods are employed for storing and recalling passwords securely?
- How are mobile devices and laptops secured, particularly when they access confidential information remotely?

By systematically addressing these questions, you will develop a clear portrait of your firm's cybersecurity landscape, enabling you to identify and prioritize potential threats. With this knowledge, you can devise a strategic plan to strengthen your defenses, ensuring your firm's sensitive data remains protected in an increasingly dangerous digital realm.

Drafting the Policy

Documenting your firm's cybersecurity plan and policies is essential, even if you are a solo firm. Documenting cybersecurity efforts constitutes part of a firm's due diligence. This policy is multi-functional and evolving. It serves as onboarding for new employees and recurring training for existing employees. It can also prove to clients that you value their privacy and actively defend their sensitive data or intellectual property.

The components of a firm's cybersecurity policy should address the following areas, but your firm may have additional concerns and require additional sections:

- Acceptable Use Policy (AUP)
- Compliance Standards
- Encryption Protocols and Secure Communications
- Adopting New and Emerging Technology
- Data Backups and Recovery
- Cyberattack Response Plan
- Training and Culture
- Insurance Coverage

Acceptable Use Policy (AUP)

The Acceptable Use Policy (AUP) is a foundational framework that outlines your firm's responsible use of technology. It encompasses all technology-related interactions, including laptops, desktops, software applications, hardware components, and mobile devices. By establishing clear guidelines, this document aims to create a secure, efficient, and productive environment for all employees while safeguarding sensitive information and maintaining compliance with applicable regulations.

The policy should explicitly address whether attorneys and staff may utilize personal devices for firm-related activities or if they are required to rely solely on devices provided by the firm. This distinction is vital in mitigating potential security risks and protecting client confidentiality, ensuring all communications and data are secured within the firm's controlled network.

Compliance Standards

Various regulations spanning multiple industries impose additional compliance requirements on law firms. The Health Insurance Portability and Accountability Act (HIPAA) exemplifies this, particularly for personal injury firms handling sensitive medical data. The implications of HIPAA compliance are profound, as non-compliance can lead to severe penalties and jeopardize a firm's credibility.

International laws such as the General Data Protection Regulation (GDPR) further complicate the data protection landscape. This regulation carries significant weight even within the legal context; for instance, court reporters now tend to follow GDPR requirements when storing sensitive client depositions even though they are not required to by U.S. federal law. However, on the state level, laws like the California Consumer Privacy Act (CCPA) echo the principles enshrined in the GDPR, mandating strict data protection measures directly affecting legal practices across the United States.

Law firms must stay abreast of these evolving regulations to ensure compliance and protect their clients and their own interests. The interplay of these local, national, and international regulations creates a complex web of obligations that requires law firms to remain vigilant and proactive in their cybersecurity strategies.

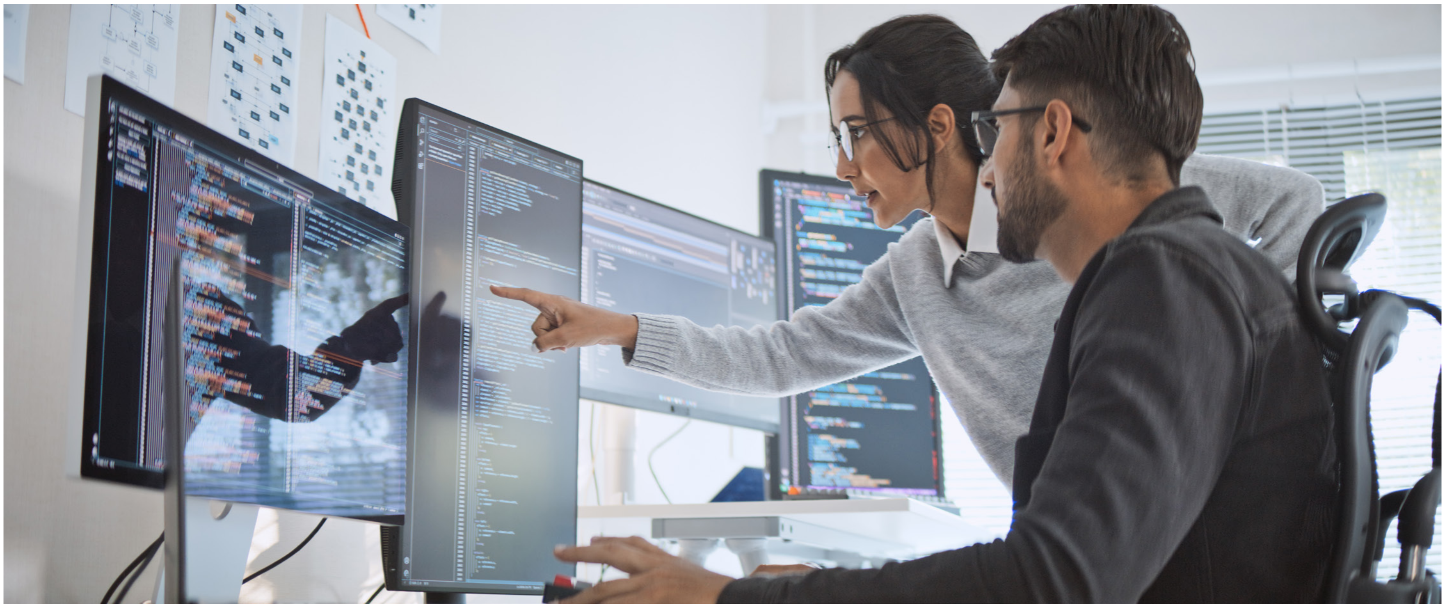
Encryption Protocols and Secure Communications

Just as you might choose a lock to protect important documents, encryption safeguards your digital data—whether files stored on your computer or communications sent over the Internet.

Encryption plays a crucial role in compliance with regulations protecting sensitive data, such as personal information and financial records. By employing encryption, you not only enhance the security of your files and communications but also align with legal requirements that protect privacy and prevent identity theft.

Additionally, your firm must use secure forms of communication. Various platforms exist for this purpose, and many can integrate multiple devices and forms of communication–calls, emails, texts–into a secure communications hub. Also, consider compliant video conferencing tools to ensure your client's remote communications remain private.

Adopting New and Emerging Technology



Keeping your firm secure requires regular software security updates (patches) and may require upgrading to the latest technology. Cloud computing is not new, but many firms have resisted cloud migration due to privacy concerns. However, cloud-based storage and other computing services are much more secure than traditional computing and have the added advantage of updating automatically.

As AI technologies become increasingly integrated into daily operations, it is crucial to delineate how and when staff can leverage such tools. Outline the best practices for using gen AI to enhance productivity while addressing ethical considerations, data privacy issues, and your firm's responsibility to maintain professional standards. For more on this subject, see our recent blog post on responsibly adopting AI.

Regardless of which technology tools your firm adopts, careful consideration must be made when implementing each tool, especially with third-party vendors. Before pulling the trigger on any new upgrades, closely examine the security features and protocols of the new service, software, or device. Do not forget to read the terms and conditions so you can clearly understand what security aspects you are responsible for with each new technology tool.

Data Backups and Recovery

A robust backup and data recovery plan is essential for any organization looking to safeguard its sensitive information and maintain operational continuity. This comprehensive document outlines the steps necessary for securely backing up critical data. It provides a clear roadmap for restoring that data in case of a breach or ransomware attack.

Secure and reliable backup services may include both on-premises and cloud-based solutions. Regularly scheduled backups should be implemented to ensure the most current data is always protected, minimizing potential loss during incidents. Encryption of backup data is paramount; even if attackers gain access to the backups, the information remains unreadable and secure.

The recovery process should be clearly defined, detailing the specific procedures to follow in different scenarios. These include identifying the breach source, assessing the damage, and executing a recovery strategy to restore data swiftly. The plan should encourage regular testing of recovery procedures to ensure readiness in times of crisis.

Draft a Cyberattack Response Plan

A cyberattack response plan details the step-by-step, moment-to-moment game plan in the aftermath of a data breach. An effective response plan requires thoroughly examining every detail surrounding a potential data breach. Below are essential best practices the ABA recommends to help you get started. Once you establish a strong foundation, you can customize your plan to align with your firm's requirements.

- **Containment**: When a breach is detected, your top priority should be to isolate the compromised systems. This protocol prevents further exposure and safeguards against the spread of viruses or malware to other networks.
- **Audit**: Meticulously evaluate the extent of the breach. Understand what data may have been exposed and confirm that no other systems are compromised.
- **Purge**: Ensure that any files affected by the breach are entirely and securely deleted.
- **Log Details**: Keep comprehensive logs of the attack. These records may serve as critical evidence should legal action be necessary.
- **Public Notice**: The ABA mandates that firms promptly inform affected individuals following a data breach.[4] Note that some regulatory bodies, like the SEC, have guidelines on when a data breach must be reported to the public, law enforcement, and regulators. Be sure to note any specific guidance in your response plan.
- **Contact Authorities**: Notify law enforcement as soon as possible. The breach may also risk other businesses or consumer groups; swift action is vital.
- **Recovery**: Develop a detailed recovery plan that defines specific roles for employees during this phase. Quick and efficient actions are crucial for minimizing damage and resuming normal operations.
- **Lessons Learned**: After resolving the incident, perform an "after-action review" with your team. Discuss what strategies worked and identify areas for improvement.
- **Update**: Commit to continually improving your systems and cyberattack response plan based on insights from past experiences and emerging threats.

Once your response plan is laid out, the next crucial step is to ensure all employees understand and effectively implement it.

Training and Culture

Each firm employee serves as the first line of defense against bad actors or as the backdoor for a ransomware attack. With the increasing quality of phishing and deepfake attacks, ongoing training is more important than ever to keep your staff working together to secure your firm's data.

The ABA recommends cybersecurity training sessions annually, if not quarterly.[2] Simulated phishing attempts or other testing can help employees stay vigilant and help the firm identify which employees need additional attention.

Beyond training, your firm must work to instill a culture of security. Encourage good cyber hygiene through strong password best practices, physical security, and rapid offboarding processes that lock former employees of sensitive systems.

Proper Insurance Coverage

Breaches can and do still occur despite the best intentions and cybersecurity efforts. The essentials are to perform due diligence by creating a comprehensive security plan and working with technology experts to lower the attack surface and mitigate risk. Additionally, your firm should have the correct type and coverage level of insurance to protect your lawyers from liability.

Protexure is here to simplify cybersecurity for your law firm and guide you in choosing the correct liability policy to navigate today's complex landscape. Contact us to discover how we can support your firm's needs.

Sources:

1. Why Law Firm Data Breaches Are Skyrocketing in 2024 | ProcessBolt
2. 2023 Cybersecurity Tech Report
3. Rule 1.6: Confidentiality of Information
4. Formal Opinion 483

Contact Us

4200 Commerce Court, Suite 102
Lisle, IL 60532

Phone: 877-569-4111
Fax: 630-799-1796
Email: info@protexure.com

Protexure

(One of The McGowan Companies)