SimpleLaw.com
Simple for Lawyers. Simple for Clients.

Protecting Your Legal Data from Cyberattacks

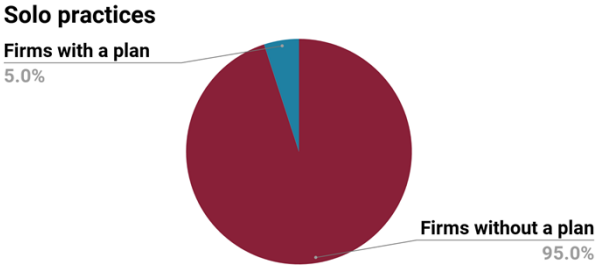
The importance of data security is at an all time high. On June 27, 2017, the most recent cyberattack, NotPetya, was unleashed. The virus freezes computers and demands a ransom to unlock them. Some big American targets include: Merck Pharmaceutical, DLA Piper, and Mondelez food company. Even more alarming, the radiation monitoring at Chernobyl was compromised.

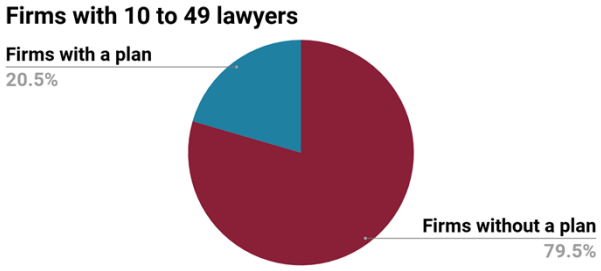
Why bring this up? This attack raises questions for law firms. Just how prepared are they for cyber breaches such as this one? More importantly, how often are law firms being attacked?

LogicForce, a leader in cybersecurity, released a report finding that law firms are unfortunately still drastically unprepared for cyber threats. In a recent study by LogicForce, over 50% of 200 law firms do not have a cyber attack response plan, and 66% reported some type of cyber infringement. 77% of the responding firms do not have cyber insurance. 95% were not compliant with their own cyber policies while 100% were not compliant with client policies.

The study has also discovered that only 5% of solo practices and 20% of firms with 10 to 49 lawyers have a plan in place. Jordon McQuawn, chief information officer of LogicForce, stated, "I don't think firm size really makes a difference."

Firms and their Cyber Security Readiness





American Bar Association Rules

The newest revision to the American Bar Association (ABA) model establishes a specific job to make practicable efforts to protect information relating to client representation. Threats affecting law firms include:

- Email phishing attacks
- Impersonation of executives
- Potential data loss
- Extortion via ransomware

New revisions to the ABA aid in protecting a firm's data and their clients

Clients themselves have been very proactive in protecting their information by taking written questionnaires, making site visits, and requesting backup evidence and testimonials. Many law firms now participate in "a legal information sharing and analysis coalition affiliated with the Financial Services Information Sharing and Analysis Center (FS-ISAC)[1]" and use numerous sources of cyber intelligence security.

A firm's general counsel should be active in participation in their data protection efforts. Their data and security programs should include compliance with International Security Standards and training for privacy and security measures.

Compliance With International Security Standards

The firm can obtain and maintain appropriate certifications, such as ISO 27001:2013. This certification covers the requirements for establishing, implementing, maintaining, and continually improving an information security management system. It also includes requirements for the evaluation and treatment of information security risks tailored to the needs of the particular organization. Practices can work directly with the ISO organization or with qualified consultants. Another option is ISO 27000:2016, providing an overview of information security management systems, and terms and definitions commonly used in the ISMS (a systematic approach to managing sensitive company information so that it remains secure) family of standards. The ISO 27000 is

The ISO 27000 aids in the protecting

- *Financial information*
- *Intellectual property*
- *Third party information*
- *Employee details*

[1] *Law360*

available to all types of commercial, government, and non-profit organizations.

Training for Privacy and Security Measures

Security and awareness training is crucial in this day and age. Providing regular phishing exercises to train your internal users is a great first step. Knowing how to identify a potential phishing scam is the first line of defense. Training your team can be done remotely through online existing sources. One such resource that provides training is TeachPrivacy. They provide privacy and data security training to companies across industries. Another resource is SecureCast, that offers a simulated phishing training program. According to SecureCast, every day 80,000 people fall victim to a phishing scam. There are over 156 million phishing emails sent globally, of which 16 million make it through spam filters, and 8 million are opened.

Prepare online with privacy and data security training

Policy and Procedures

Policies should establish the proper use of a firm's technology resources, including the use of social media, and the protection of important personal information. There are countless resources from free downloadable templates to various consulting firms. Many legal marketing and PR firms can assist practices as well.

The American Bar Association (ABA) offers it's members many resources to help develop technology use policies and procedures. LexisNexis also offers books to help develop the guidelines. Additionally, there are a multitude of consultants and PR firms that can help look for a consultant who has expertise in data security and law firm management.

Some PR firms offer free downloads. They can also provide specific plans for your firms based on your precise practice setup and concerns.

The American Bar Association offers comprehensive models for:

- *Social media policies*
- *Document retention policies*
- *Disaster recovery plans*
- *Incident response plans*
- *Mobile security policies*

Business Continuity

Preserving a business continuity and a disaster recovery program, for potential future events, is of the utmost importance. Programs can include governance, testing mechanisms, and system documentation to prepare for unseen problems. The American Bar Association provides many resources that firms can use in case of a disaster. The ABA Legal Technology Resource Center (LTRC) can help your firm in disaster preparedness including best practices for computer backup and disposal, business continuity, checklists for disaster preparedness, tech resources for disaster relief, a checklist to get your practice up and running after a disaster, hotline for consultations, and information on local and national technology resources. The guide provides information regarding disaster planning and recovery for law firms, law practice management resources, and lawyer assistant programs.

Business continuity plans provide a supporting base in case of disaster

Internal Security

Internal protections are necessary to combat cyber attacks. Adding endpoint security agents, firewalls, and internal intrusion detection sensors are the first priority. There are many resources to help a firm choose these tools and implement them. The ABA offers a book titled Cybersecurity Handbook. The guide offers practical cyber threat information, guidance, and strategies to lawyers and their law firms on how to defend against a threat, but also provides advice on the best way to respond if a breach occurs. The Digital Guardian has an extensive list of legal data security experts who discuss technologies and processes to protect your clients' sensitive information.

Internal protection techology guards client information from security breaches

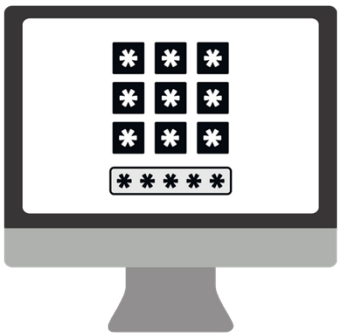
Physical Security

Physical security cannot be overlooked. Measures such as keycard access, security cameras, and requiring visitors to have an ID should all be considered. For people working with the practice either remotely or in the office, there should be password requirements, settings for user account inactivity, session lockouts, and account disability. The Cyber Advocate website provides a free download for a physical security checklist. With said checklist, one can receive access to records of the most common physical security risks in a modern law firm, which are divided into categories, including human, environmental, and supply system lists. Cyber Advocate's own rating system, responding to your checklist entry with a "good," "caution," or "warning" rating, letting a firm know where to focus their security efforts.

Protect your clients and your practice by taking physical security measures

Encryption

There needs to be policies for encryption, password complexity, and tracking for phones to enable remote mobile lock and prevent data loss. Mobile lock, or SIM lock, is a technical restriction built into mobile devices by the manufacturers to restrict the use of the phone in certain countries or networks. Mobile devices should be encrypted in general. Firms need to periodically perform vulnerability scans as well. Encryption is required of all transmitted records and files containing personal information that will travel through public networks, and also for all data containing personal information that is transmitted wirelessly. Encryption is necessary for personal information used on portable devices. The ABA has a must-read article titled, Encryption Made Simple for Lawyers making encryption easier to understand. The ABA also has a list of possible sources to get encryption software with email, system, and mobile storage encryption as options.



Secure online data through encryption

Summary

Attorneys have a responsibility for their data. The first line of defense is the user accessing data over the web or cloud. Ensuring you and your team are educated on what potential scams can look like and what to do if one is seen is a minimum requirement.

Beyond the user, ensuring data is secure from hackers or malware is the next step. There are endless resources available that are reasonably priced to install data security tools including McAfee®, Entrust(R) and more.

Advanced persistent threats (APTs) are a form of a coordinated hacking attack. These threats can come from hackers, cybercriminals, economic spies, and dishonest unfavorable parties. There are no signs that these efforts are stalling or decreasing. In fact, as the world becomes more connected, the greater the threat.

Attorneys have worked hard to not only become lawyers but to build a practice. Although technology is making case and practice management more simple, it also introduces potential threats. With a little time, study, and organization, these threats can be quickly diminished.

Protect your practice from malware or phising attack, and secure your data