McGowan Program Administrators

7 Security and File Privacy Best Practices for Lawyers

Security and privacy hazards haven't changed with advanced technology, but the means of loss have. Before the days of personal computers and the internet, lawyers always had possession of their clients' personally identifiable information, trade secrets, and other confidential information.

An attorney has the duty to safeguard information from unlawful and wrongful distribution and maintain it so it remains accessible for the purposes intended. If a claim should arise due to the loss or wrongful distribution of information, it would be treated as a violation of the standard of care and as a claim for malpractice.

Lawyers hold a wealth of confidential client information that makes an attractive target for criminals:

- Social Security, bank account, and credit card numbers
- Personal, professional, and business financial data
- Medical records
- Intellectual property and trade secrets

Because these records are often stored and transmitted in digital form, it's crucial to keep them out of reach of hackers and online criminals. Wrongdoers no longer need to be physically present in the attorney's office to take or destroy sensitive information. However, if a hacker steals data, the essence of the allegations against the attorney remains the same — failure to comply with the duty to safeguard the client's information — malpractice.

Many Lawyers Professional Liability (LPL) carriers have addressed this issue in a way that limits their exposure — they may offer coverage, but cap their responsibility at less than the full limits of liability on the policy. Instead of trying to limit liability, however, McGowan Program Administrators underwrites policies to specifically include these risks.

This eBook from McGowan, expert developers of LPL policies, will help attorneys navigate the fundamentals of information security.

We spell out seven best practices that can help lawyers:

- Reduce the likelihood of losing confidential data to digital criminals.
- Manage the potential risks of losses from malpractice, negligence, or breach-of-contract claims.
- Enhance compliance with strict state and federal data-privacy requirements.

Let's dive into the checklist.

1. Establish physical security

With news reports sounding the alarm on ransomware and massive data breaches, it's easy to overlook the basics: securing the physical premises of your law office and everything inside it.

Ideally, your law office should include a security system with intrusion alarms, theft-resistant door locks, and 24-hour video surveillance. Make sure file cabinets have locks. Establish protocols for locking down confidential files rather than leaving them on people's desks overnight.

You can't assume everybody in your building is authorized to be there. You should assume, however, that criminals will be brazen enough to enter your office and steal anything valuable that's easy to find.

2. Strengthen defenses against computer and network intrusions

Security experts call it perimeter defense: using hardware and software to discourage intruders from breaking into your networks and computers. Perimeter defenses include:

- Firewalls to control data flowing into and out of your network.
- Intrusion detection technologies that scan for anomalies in your network traffic and send alarms when something is amiss. These tools can include hardware and software.
- Virus protection software. Digital criminals often use computer viruses to gain unauthorized access to IT systems. Virus protection software can scan for malware and other nefarious applications and flag them before they cause substantial damage.

Weaknesses in any of these defenses can cause havoc.

3. Keep virus definitions up to date

Technology providers like Microsoft and Symantec keep a running list of virus definitions that flag new threats and help plug security holes. Because new threats arrive on the scene constantly, updating your virus definitions is a core function of information security.

You have to figure out how often to update your virus definitions. The most straightforward strategy is to accept all updates when they arrive from your software or hardware provider. However, there may be reasons to have a different update strategy, whether it's hourly, daily, weekly, or monthly.

You'll have to confer with your IT experts to find the most reasonable definition-update schedule.

4. Keep operating system and application software up to date

Operating system and application providers deliver regular updates to patch security vulnerabilities. It's imperative to patch the current versions of your operating system and applications as soon as possible — preferably when the provider makes the update available.

A thornier question is whether to update to new versions of your software. These so-called upgrades often present a morass of usability and compatibility challenges that generate a storm of user complaints.

Resistance to version-level updates encourages procrastination in many organizations. Unfortunately, delaying these updates places you at greater risk because intruders are always on the prowl for older software with known vulnerabilities.

5. Enforce a strong password policy

Password policy starts with your IT administrators. They must be required to change all "default" passwords in applications because these are easiest for hackers to guess. All new users need to create a unique password when they open their account.

Your IT staff also can deploy an application that scans for duplicate or easy-to-guess passwords.

There's considerable debate over whether to create overly complex passwords that must be changed regularly, such as every 90 days. While these efforts are superior to easy-to-guess passwords that never change, hackers can circumvent these protections.

Many experts recommend using a long passphrase that is easy for the individual user to remember but difficult for a hacker to figure out. Also, consider using password-manager software that can provide unique passwords for every site a user visits.

6. Encrypt all confidential data

IT security experts are fond of saying there are only two kinds of organizations: those that have been hacked and those that don't know about it. Resourceful hackers can find a way into almost any system — but you can make it difficult for them to steal anything valuable if they get inside yours.

Encrypting sensitive, confidential information scrambles it into a code that makes it useless to anyone who lacks the decryption key. Data must be encrypted in three phases:

- Storage: Encrypt confidential information stored on in-house computer systems and mobile devices like smartphones and tablets. Protecting stored data ensures that somebody who steals a device or computer cannot access the data without a passkey. Furthermore, it thwarts any invaders who find their way into your systems. Note that stored data can be encrypted in multiple ways, each with distinct pluses and minuses. You'll have to consult closely with your IT experts to make sure you understand how your encryption works.
- Transmission: Apply encryption to data transmitted over your wired network, the internet, and Wi-Fi. Because email is the most common target of hackers, it's essential to encrypt emails during transmission. You also need to know the basics on common encryption formats used in transmission:
    - WPA/WPA2/WPA3 — Wi-Fi Protected Access. Wi-Fi equipment uses these protocols to encrypt wireless transmissions; version 2 is more secure than the first one. WPA3, announced in January 2018, will provide even more security.
    - IPSEC — Internet Protocol Security. IP networks use this protocol to encrypt their traffic. Most internal business networks use IP.
    - SSL — Secure Sockets Layer. This protocol allows a server to create an encrypted connection with a web browser, which is essential to secure eCommerce over the web and mobile devices.
    - PEAP — Protected Extensible Authentication Protocol. This protocol provides beefed-up security on wireless devices.
- Backup: Your data backups also require encryption protection. Moreover, backing up your data locally and to a remote site is a crucial component of IT security. Ransomware attacks, for example, usually target on-site backups, but they're much less effective against remote backups. Backups should happen at least daily, but you should look into the possibility of multiple backups during the day as well. Note that your backup and recovery program requires thoughtful design, thorough documentation, and robust testing to ensure it will perform as needed in a crisis.

In theory, hackers could figure out how to access your decryption key and descramble your data. But they're more likely to seek out softer targets once they realize they cannot find any data worth stealing in your systems.

Of course, encryption is not a cure-all. Applications that access encrypted data may have vulnerabilities that hackers can exploit, for instance. Take time to research the limits of encryption at the storage, transmission, and backup stages.

7. Learn from previous breaches

Create an assessment of previous intrusions and figure out what went wrong. Write a report documenting:

- **Where the invasion happened.** A co-worker's stolen laptop or a client's lost phone could be the avenue hackers chose.
- **How much was lost.** The magnitude of the losses should tell you what criminals are looking for and where you need to focus your efforts.
- **Why it happened.** It's rarely one thing. It's usually a chain of small oversights that create large opportunities for hackers.
- **How it could have been prevented.** Take a hard look at each stage of the breach and ask yourself what you could've done better.

All these lessons can help you elevate your security policies and practices. If you haven't been breached — and a thorough analysis of your systems finds no intrusions — explore the facts on other law firms that got hacked. Here are three examples:

- The massive Panama Papers data leak explained (Computerworld)
- 6 major law firm hacks in recent history (ABA Journal)
- The Con of Social Engineering: Law Firms are Easy Prey (New York Law Journal)

Insuring against the loss of confidential client data

While the details may have changed since the 1970s, the essence of security and privacy practices today remains the same: it is the duty of the attorney to safeguard the client's data.

An LPL policy from McGowan Program Administrators can help you manage the risks of a security and privacy breach. We provide errors and omissions (E&O) coverage to:

- Sole proprietors and law firms from 1 to 99 attorneys.
- Solo attorneys who practice law part-time.
- Solo attorneys working in a non-legal job and need insurance for "moonlighting" as an attorney.

We can customize coverage to suit a diverse range of law office requirements. We can match premiums, deductibles, limits, and other features to your precise needs and budget.

In our application, we ask a series of questions designed to determine whether an applicant understands the risks involved — both physically and virtually — and takes (at least) a minimal effort to safeguard the client's data.

If it is clear the applicant is taking this obligation seriously, McGowan is willing to insure against the hazard and offer applicants a discount on their premiums if they're abiding by the best practices in this eBook. Download this application for coverage and see how you fare on a series of questions about the strength of your security practices.

Contact us:

McGowan Program Administrators
20595 Lorain Road
Fairview Park, OH 44126

Neil McGowan Esq., M.B.A. | National Program Director — Lawyers Professional Liability
nmcgowan@mcgowanprograms.com
P: 800.545.1538 x3651