A LEGAL OFFICE MANAGER’S GUIDE TO PREVENTING TECHNOLOGY HEADACHES

WWW.JMARK.COM
Downtime, compromised data, security breaches, and slow-running technology can cause big headaches for a modern law office. After all, time is money, and when you bill by the hour every minute counts.

You can’t afford for anyone in the office to sit idle waiting for your technology to work. If your competitors are using the latest I.T. solutions, they’ll blow right past you and take clients away, or worse, the firm may lose a case, causing your reputation to suffer.

Technology helps your attorneys and employees carry out essential tasks, exercise professional judgment, engage with and represent clients, provide advice, and settle key commercial dealings. If you view technology as an opportunity and enabler rather than a necessary evil, the firm will prosper and reap the rewards. If you don’t, you’ll fall behind competitors who have embraced it.
Your firm uses technology now more than ever, or at least it should be doing so. Today’s technology is invaluable, and with time, it will become even more so. In the past, the legal profession lagged behind others in the adoption of new technology. Lawyers relied on law books and paper documents, but this is no longer the case.

Law offices are embracing new technology. Just like other businesses, you need to streamline services and introduce efficiencies to save time and process information. So technology like electronic case organization, electronic spreadsheets, databases, word processing, legal research software, presentation applications, and e-billing software have all become indispensable.

**However, along with the benefits, come the challenges.**

Failed backups, slow running email, application problems, and operating system crashes create headaches that hamper everyone’s productivity.

Downtime is a threat and can result in a major loss of productivity. Time is precious. Who can afford server failures, poor system performance, accidental file deletion, or a software application that constantly crashes? Without data access, no one can do their job or meet their deadlines. An hour lost is money gone forever.
Data security is an issue. Client confidentiality is your most sacred trust. But with hackers and outsiders who want to infiltrate your environment, your firm’s technology landscape can be a minefield unless it's properly protected. If your clients’ confidential data is stolen, you'll face penalties, fines, and possibly civil prosecution.

**THE ANSWER IS TO CONTRACT WITH THE RIGHT MANAGED SERVICES PROVIDER**

To prevent I.T. headaches, you need service and support from an I.T. provider who knows about the line of business (LOB) applications law firms use. One who understands the billing systems, document management, PCLaw, Worldox... and all other technologies that help you ensure efficient operations.

The right provider can ensure these systems seamlessly incorporate with other applications in use, like Microsoft Office 365 programs. When you have the expertise from a managed service provider (MSP) who truly understands your unique needs, you can effectively leverage these powerful tools and rest assured your I.T. is in professional hands.

**Look for an MSP who has been serving the needs of law firms and corporate legal departments for years. One who can cover a broad range of technology requirements through both professional services and managed I.T. services, and who can grasp the complexities your firm faces.**
An MSP should be able to help you avoid I.T. headaches by helping implement solutions that automate routine legal transactions, share documents and work processes, deploy mobility solutions, and capitalize on tools like electronic data discovery.

A modern law practice requires a complete technology management solution, including data protection and proactive monitoring of all key functions on your network, servers, and workstations. Furthermore, you should insist upon a fixed-cost solution and predictable I.T. budgeting. Just as your firm’s attorneys are committed to the rights of their clients, your MSP must be dedicated to making you successful. You should view each other as partners. An excellent MSP will become an extension of everything your firm does.

Your MSP should be adept at:

**Cloud technologies** that improve your business productivity, efficiency, and security. With cloud solutions, you can eliminate the cost of paper and the hassle of sifting through files, store massive amounts of information (a.k.a. “big data”), share important files in real time, and secure your clients’ information offsite in high-security data centers.

**Case management software** that brings your staff’s desktop calendars, contacts, filing system, and task-management solutions together in one package. This solution helps all attorneys and employees better organize, manage deadlines, retrieve client information, and coordinate communications. In addition, case management software provides the firm with proactive data that helps you to effectively manage the business and offers feedback on how you’re progressing.
Financial management software to help you manage billable hours, design short- and long-term financial plans, and budget expenses accordingly. Your MSP should be able to train your employees on financial management software specifically designed for law firms.

THE WORST HEADACHES RESULT FROM I.T. SECURITY BREACHES

Data breaches are increasing exponentially. Cybercriminals have moved into small towns and often operate from legitimate-looking offices. Hackers are no longer kids in their parents’ basement working on a few computers. Cybercrime is an international and sophisticated business with cartels operating around the globe.

Data is valuable, and every law firm is a target. However, I.T. security best practices change rapidly, and law firms often find themselves lagging behind the I.T. security curve. If you fall behind, your firm is at risk. Viruses, network vulnerabilities, or data breaches can cause much more than a headache—now you’re looking at a full-blown migraine! This is why you need the expertise of an MSP who understand the threat landscape and stays on top of the latest happenings. It’s imperative that you protect client and case information.
Criminals have many ways of stealing your data.

**Internet Exploits**
Your employees use connected devices to interact with, track, monitor, and simplify just about every area of their work and personal lives. However, these technologies also provide access to sensitive, confidential information, and can contain a wide variety of new security vulnerabilities attackers could exploit.

**Third-Party Attacks**
Cybercriminals have learned that contractors and other third-party providers aren’t as secure as large vendors; they know that this lower security provides a pathway into otherwise-secured networks. Examine who has access to your network and confidential information, even if you believe appropriate security measures are in place.

**Social Media Attacks**
Social media presents two main security headaches:

1. A website you visit or service you use can be infected with malware that spreads, putting your network at risk for a data breach. Malicious social media content is expected to grow 400 percent, as attackers continue to distribute their malware and steal data.

2. A determined hacker or team can scrape social media sites to assemble a surprising amount of personal data very quickly. This data can be used to social engineer an attack.
Social Engineering Attacks
Human nature is easily the weakest link in any security chain. Was that really a utility company employee you held the door for this morning? Are the painters you hired propping open a secure door to make their task easier? Did your receptionist just give all of her passwords to someone who called up claiming to be from tech support? Will someone’s curiosity cause him to insert the USB drive he found in the parking lot into his computer?

Mobile Malware Threats
Security experts have been warning about mobile malware threats for a long time, and users have grown immune to these warnings. Mobile device use is increasing, as is the sophistication of attacks. Data shows that with each new year, a major mobile malware attack is increasingly more likely to occur. Attackers typically select the greatest number of potential victims. So, they will target well-known mobile devices—most likely Android and jailbroken iOS devices.

Sophisticated DDoS Attacks
Distributed Denial-of-Service (DDoS) attacks don’t directly steal your information. Instead, they overwhelm your site or service with so much traffic that it prevents legitimate users from connecting. These attacks have evolved beyond simple flooding of traffic. They probe and then morph, based on the defenses in place on your network. Such advanced and sophisticated attacks can seriously impair your law firm’s ability to operate.
TO PREVENT THESE SECURITY HEADACHES YOU NEED A SECURITY PLATFORM WITH REMOTE ACCESS MONITORING AND A RELIABLE BACKUP AND DISASTER-RECOVERY SOLUTION

Make sure your I.T. provider implements innovative, up-to-date security measures to protect your network against intruders, malware threats, and disasters. Make sure they can do the following:

**Ensure:**

- Everyone complies with all legal and confidentiality requirements when using technology.

- Appropriate technical means are used to minimize the risk of disclosure, discovery, or interception of communications.

- Data and email are encrypted to protect all sensitive information.

- The firm adopts management practices that offer protection against disclosure or discovery of electronically transmitted messages.
Prevent:

• Unauthorized access to all electronic data.
• Computer viruses from damaging data.
• Natural or manmade disasters from affecting I.T. operations.

Confirm:

• All files are reliably backed up and recoverable.
• Both offsite and onsite data backups are maintained.
• Data is restorable by performing ongoing testing.

Provide:

• Systems analysis.
• Mobile device management (MDM).
• Up-to-date security solutions.
• User support and training.

Your MSP should implement a security platform with multiple layers of protection, and 24/7 remote monitoring to detect infections and intrusions and block them before they can compromise systems or data. A good MSP should keep you informed and train your staff to recognize threats, so every user knows what to do if a threat comes across your computer screen.
The most basic security solution should include barriers with virus and malware detection at the firewall level, and with DNS (Domain Name Server) controls to ensure users don't visit hijacked websites. Every user should also practice two-factor authentication access to prevent criminals from getting into the network using lost, stolen, or compromised passwords.

Nothing is more important than protecting the information on your network and having the peace of mind that comes from knowing that you can fully recover if a disaster hits your firm. Your MSP must ensure that your business continuity and disaster recovery solutions meet best practices by implementing a robust backup and secure off-site replication solution.

While computer systems can easily be replaced, the intellectual property and sensitive information stored on those systems cannot. Computer hard drives can fail, laptops can be stolen or lost, and data can be erased due to human error or viruses. It's important for your firm to have a backup system, to keep data safe and avoid data loss.

Ask your MSP if they employ system virtualization and a private cloud with a fully redundant system that can be replicated across multiple data centers. If data is compromised or damaged, a new clone of your system and data can be spun up with a fresh image in a matter of seconds.
Be sure your managed service provider uses an intrusion detection system. This platform can catch any malicious attempt that may have bypassed the firewall. Intrusion detection can either be used to catch a break-in attempt in progress or to detect one after the fact. In the latter case, it's too late to prevent any damage, but at least you'll be aware of the weakness that was exploited.

If an intruder gets into your system, the first thing they typically do is install a rootkit. A rootkit is a script or set of scripts that can make changes to your I.T. system and hide in common system utilities. They function in the background without you knowing they are there. Criminals can easily obtain these on the internet. This is another reason why you must have reliable backups of your entire I.T. system. If rootkits are discovered, you'll need to re-install your system and data and start from scratch.

All mobile devices also need monitoring and management. If a phone or laptop is stolen, you must be able to remotely wipe any and all confidential data. Mobile device management also prevents disgruntled employees from leaving with confidential or proprietary data.

Your MSP should also employ encryption to protect your confidential data. They should encrypt emails and data to ensure the security of information. Encryption can protect your data at rest, such as on laptops or portable servers, as well as data in motion, while it is being transmitted over wireless networks or the internet.
One of the most overlooked security aspects in law firms is archiving and retention policies regarding email and data. You need to be accountable for instituting and employing a strategy that details the duration for which your client data and emails will be stored and deleted. Make sure your MSP can implement automated solutions to handle this for the firm.

**IN CONCLUSION**

A good office manager understands the unique challenges and technology demands the modern law firm faces. Whether your I.T. headaches come from the security risks of handling and storing confidential information, or the difficulties of keeping up with new, innovative line-of-business solutions, you need an I.T. provider who can ease your struggles and your I.T. headaches.

JMARK has been helping law firms of all sizes capitalize on business technology for thirty years. Would you like a no-risk I.T. Strategy Review that will leave you with the knowledge you need to execute on the strategies in this book? One that will help you understand how to increase the maturity of your I.T. environment, which will help you enhance the performance of your firm? **To arrange a free I.T. Strategy and Review session, contact Todd Nielsen at 844-44-JMARK or Todd@JMARK.com.**