Veltec Networks

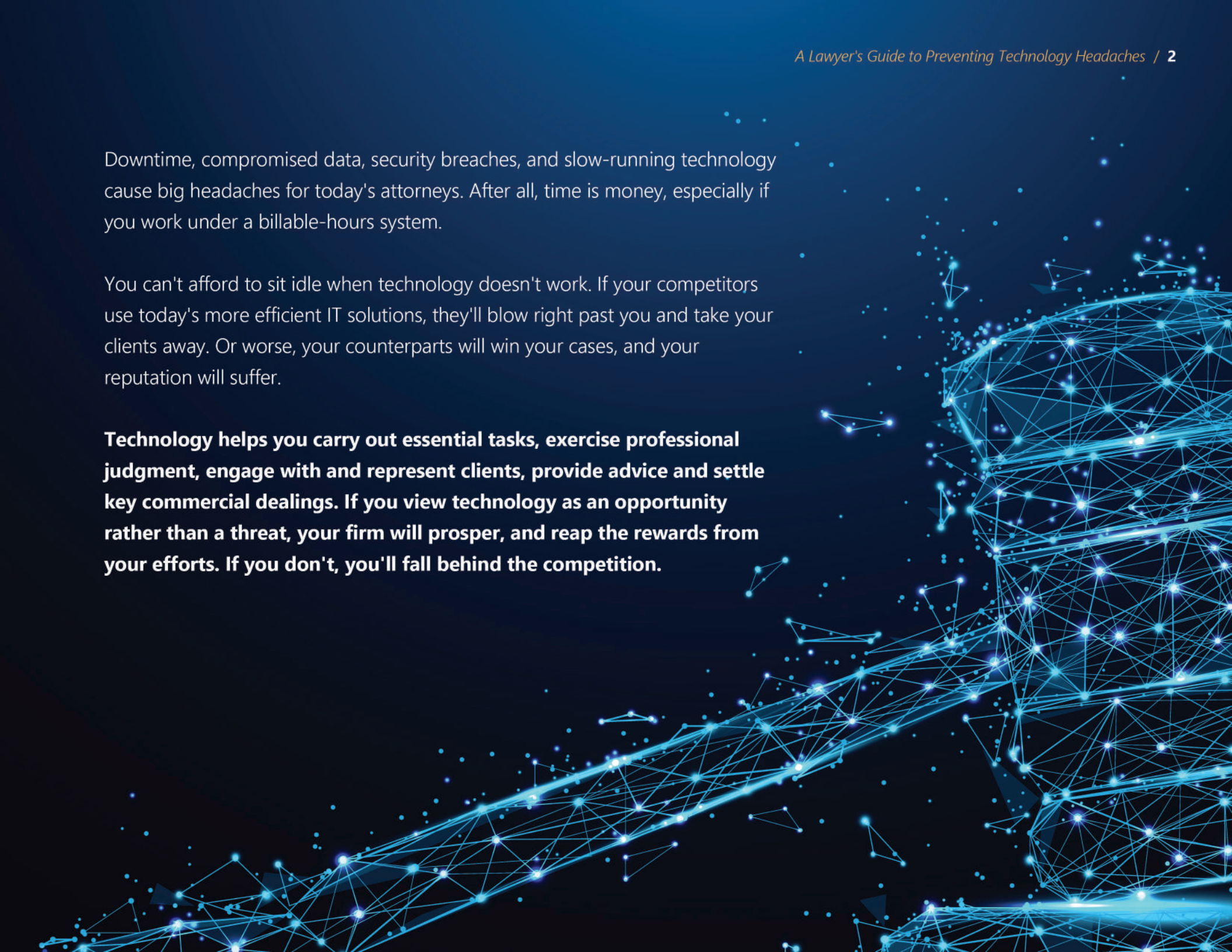
A Lawyer's Guide to

Preventing Technology Headaches

Downtime, compromised data, security breaches, and slow-running technology cause big headaches for today's attorneys. After all, time is money, especially if you work under a billable-hours system.

You can't afford to sit idle when technology doesn't work. If your competitors use today's more efficient IT solutions, they'll blow right past you and take your clients away. Or worse, your counterparts will win your cases, and your reputation will suffer.

Technology helps you 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 rather than a threat, your firm will prosper, and reap the rewards from your efforts. If you don't, you'll fall behind the competition.



You use technology now more than ever – at least you 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 with the adoption of new technology. They relied on law books and paper documents, but no longer.

Law offices like yours are now embracing new technology. Just like other businesses, you need to streamline services to save time and process information with technology like electronic case organization, electronic spreadsheets, databases, word processing, legal research software, presentation applications and e-billing software.

However, along with the benefits technology provides, come challenges.

Failed backups, slow running email, application problems and operating system crashes create headaches that set up barriers to your success.

Downtime is a threat. Downtime will result in a major loss of productivity. You can't afford to be presented with server failures, poor system performance, accidental file deletion, a software application that crashes. Without the data access, you and your employees can do your jobs. Money goes out the window, and you can't meet your deadlines.

Data security is an issue. Client confidentiality is your most important duty. But with hackers and outsiders who want to infiltrate your technology for their own legal purposes, your technology landscape will be like a minefield unless it's properly protected. If your clients confidential is stolen, you'll face penalties, fines, and possibly civil prosecution. You can't take this chance.

THE ANSWER IS TO CONTRACT WITH THE RIGHT TECHNOLOGY SERVICES PROVIDER

To prevent IT headaches, you need the service and support from an IT Provider who knows about the Line of Business (LOB) applications you use. One who understands your billing systems, document management, PCLaw, Worldox and other technologies that ensure your efficient operations.

The right provider can ensure these seamlessly incorporate with other applications you use like Microsoft Office or Office 365. When you have the expertise from a Technology Solutions Provider (TSP) who truly understands your needs you can effectively leverage these powerful tools.

Look for a TSP 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 IT services and that can grasp the complexities your law firm faces.

They should be able to help you avoid IT headaches when automating routine legal transactions, sharing documents and work processes, deploying mobility solutions and capitalizing on tools like electronic data discovery.

Your law practice requires a complete technology management solution including data protection and proactive monitoring of all key functions on your network, servers, and workstations. Plus, you should insist upon a fixed-cost solution and predictable IT budgeting. Just as your attorneys are committed to your clients' success, your TSP must be dedicated to making you successful and view themselves as partners, and an extension of your practice.

Your TSP should be adept at:

Cloud Technologies that improve your productivity, efficiencies, and security. With our cloud solutions you can eliminate the cost of paper, the hassle of sifting through files, store massive amounts of information (Big Data), share important files in real time, and secure your clients' information offsite in our 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 helps you and your employees better organize, manage deadlines, retrieve client information, and coordinate communications. In addition, case management software provides you the proactive advice you need to effectively manage your law practice and feedback on how you're progressing.

Financial Management Software to help you manage your billable hours, design short- and long-term financial plans, and budget your expenses effectively. They should be able to train your employees on Financial Management Software specifically designed for law firms.

THE WORST HEADACHES RESULT FROM IT SECURITY BREACHES

Data breaches are increasing exponentially. Cyber mafias have set up in towns like yours and operating 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.

Your data is valuable, and your law firm is a target. You need the expertise of a TSP who stays up to date on the latest threats. It's imperative that you protect client and case information. But IT security best practices change rapidly, and law firms often find themselves falling behind the IT security curve. If you do, your firm is at risk for viruses, network vulnerabilities, or data breaches. This results in more than a headache; now you're looking at a migraine.

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 present a wide variety of new security issues for attackers to exploit.

Third-Party Attacks

Cybercriminals have learned that contractors and other third-party providers aren't as secure as large vendors, and lower security provides a pathway into otherwise-secured networks. Examine who can connect to your network and access 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 until your network is ripe for a data breach. Malicious social media content is expected to grow 400 percent, as attackers continue to distribute their malware and steal client 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 your office painters propping open a secure door to make their task easier? Did your receptionist just give all of your and her passwords to someone who called, claiming to be from tech support on another floor? Will your colleague's curiosity cause him to insert the USB key he "found" in the parking lot into his computer?

Mobile Malware Threats

Security experts have been warning us 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. At the risk of being the boy who cried, "Wolf," every year a major mobile malware attack is now more likely to occur. Attackers typically select the greatest number of potential victims. So, they will target mobile devices, specifically Android and jailbroken iOS devices.

Sophisticated DDoS Attacks

Distributed Denial-of-Service 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 operations.

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 Technology Solution Provider implements innovative, up-to-date security measures to protect your law practice against intruders, malware threats, and disasters. And make sure they can do the following.

Ensure:

- You comply with legal and confidentiality requirements when using technology.
- You use appropriate technical means to minimize the risk of disclosure, discovery, or interception of communications.
- Data and email are encrypted to protect your sensitive information.
- You adopt management practices that offer protection against disclosure or discovery of electronically transmitted l messages.

Prevent:

- Unauthorized access to your electronic data.
- Computer viruses from damaging your data.
- Natural or manmade disasters from affecting your IT operations.

Confirm:

- Your 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
- Up-to-Date Security Solutions
- User Support and Training

Your TSP 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 and get in and steal or hold your data hostage. Many law firms are unaware that this goes on. Your TSP will keep you informed and train your staff to recognize threats, so you know what to do if one comes across your computer screen.

Your very 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 your users don't visit hijacked websites. Your employees should also practice two-factor authentication access to prevent criminals from getting into your network.

Nothing is more important than protecting the information on your network and the peace of mind that comes from knowing that you can fully recover if a disaster hits your firm. Your TSP must ensure your business continuity and disaster recovery solutions will meet your objectives and implement 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 TSP if they employ system virtualization and a private cloud with a fully redundant system that can be replicated across multiple data centers. If your data is compromised or damaged, a new clone of your system and data can be spun up with a new fresh image in a manner of seconds.

Be sure your Technology Solutions Provider used an Intrusion Detection System. This will catch anything that may have bypassed your firewall. They 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 problem.

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 IT 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 one reason why you must have reliable backups of your entire IT system. If rootkits are discovered, you'll need to re-install your system and data and start from scratch.

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

Your TSP should also employ encryption to protect your confidential data. They should encrypt both your 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, such as over wireless networks or the Internet.

One of the most overlooked security aspects in law firms is their archiving and retention policies regarding email and data. You are 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 TSP can implement automated solutions to handle this for you.

IN CONCLUSION

You understand the unique challenges and technology demands your law firm faces. Whether your IT headaches come from the security risks of handling and storing confidential information, or the difficulties from keeping up with new, innovative Line of Business Solutions, you need a Technology Solutions Provider who can ease your struggles and your IT headaches.

Veltec Networks

For more information, contact us at
(408) 849-4441 or info@veltecnetworks.com.