Seven Common Technology Mistakes by Law Firms

By Matt LaMaster

In today's ultra-competitive and fast-paced society, increased billable hours and heightened client expectations dominate the practice of law. For most of us, that leaves little time for much else. Law firms and attorneys must concentrate their time and energy on their clients. After all, that makes good business sense. However, too often that means disregarding effective technology practices.

Many firms don't have the resources or appetite to stay up to date with the latest technology news, security threats, and constant changes that impact their business. Additionally, not all attorneys and firms are adept at maintaining best technology practices, and as a result, commonly disregard crucial technology procedures. Over the past few years, I've made a list of the mistakes I've encountered firsthand in law firms. I've also jotted down some basic fundamentals and tips to fix those mistakes and allow your law practice to stay ahead of the curve. Below is a list of the seven most common mistakes and some essential measures to help protect your firm.

1. Insufficient technical support

Realizing when a firm is receiving inadequate technical support is generally not difficult. Unfortunately, the mistake often has major consequences.

Some firms continually struggle to find sufficient technical support. Others simply forego professional support, believing it's too expensive. As a result, many rely on a young attorney or paralegal whose knowledge of Microsoft Word may make him or her the firm's "computer guru." Others may depend on a friend or relative who moonlights as an "IT guy" to provide technology advice or assistance when critical systems fail or slow to unacceptable levels.

Some firms hire a professional who provides services on a break/fix business model, which follows this framework: IT issues occur (severe or standard), the firm calls the IT guy, and waits and wonders how long it will take for a response and how much it will ultimately cost. Unfortunately, this model is extremely outdated, unreliable, and tremendously difficult to budget.

Law firms need knowledgeable, trusted technology partners who proactively monitor and manage their technology and understand their specific operational requirements. The result is a more efficient and profitable law practice. Ultimately, that means fewer headaches for everyone involved.

Here are a few items you should look for in a technology provider:

- They understand law firm operations.
- They understand Rule 1.6 of the Michigan Rules of Professional Conduct as it relates to technology and will agree to a confidentiality agreement. You should also make sure they understand other specific compliance requirements.
- They provide managed services by proactively monitoring and fully managing your systems and network.
- They provide unlimited phone support for your entire team for IT issues.
- They securely provide local and cloud backup services and document the security protocols for these services.
- They provide a managed security suite for all workstations and servers.
- They act as trusted partners and advise you on cost-effective technology solutions.

Law firms need knowledgeable, trusted technology partners who proactively monitor and manage their technology and understand their specific operational requirements.

Law Practice Solutions is a regular feature brought to you by the Practice Management Resource Center (PMRC) of the State Bar of Michigan, featuring articles on practice management for lawyers and their staff. For more resources offered by the PMRC, visit our website at http://www.michbar.org/pmrc/content.cfm or call our Helpline at (800) 341-9715 to speak with JoAnn Hathaway or Diane Ebersole, Practice Management Advisors.

I often go into firms and see an assortment of systems from Dell, HP, and Lenovo. The resulting mishmash increases costs and complicates troubleshooting, repair, and deployment.

2. Hardware issues resulting from inconsistent systems

The second most common technology mistake firms make is failing to standardize hardware systems. I often go into firms and see an assortment of systems from Dell, HP, and Lenovo. The resulting mishmash increases costs and complicates troubleshooting, repair, and deployment.

Many organizations set hardware service lives at three or four years. There's a reason, and it's not because they have huge budgets. It's because they see the benefits of having a standardized platform.

"When you look at hardware costs—particularly when overextending a computer to a five- or six-year life cycle—it may seem like you are saving money," says Barron Henley, a partner at Affinity Consulting Group. "But really it's costing you."[1] That's because support expenses can increase when you keep computers longer than four years. Even worse, older and obsolete hardware is less efficient, increases the likelihood of down time, feeds employee frustration, and can threaten client care. Law practices can overcome common hardware issues by retiring equipment at proper life cycles—typically three to four years—and working regularly with a reputable technology partner to help ensure that consistent, high-quality hardware is being deployed throughout the firm.

3. Insufficient training

It's estimated that most employees understand less than 20 percent of the available features in the software applications they use. That means 80 percent of the features, time-saving capabilities, and cost-reducing functions remain unused.

To remedy this problem, it's imperative that law firms identify technology partners, onsite training firms, and other programs to assist in maximizing software applications. It's really quite simple—if you skimp on training, you end up with technology that is underutilized or inefficiently used, leading to frustration and, ultimately, wasted money.

4. Security failures

Law firms frequently fail to recognize and fully protect against security risks. And they don't need to be high profile to be targeted; by nature, law firms are targets. You probably know there are unscrupulous hackers constantly scouring the Internet in search of poorly secured servers, computers, and networks to infect and exploit, and law firms are victimized every day. As a result, those that fail to properly secure their networks may find themselves in the middle of a crisis resulting in bad press, lost clients, and ethical inquiries by the state bar association.

Fortunately, some simple steps can help prevent security failures:

- Implement and enforce strong password security policies.
- Ensure that your operating system is current and security updates are installed.
- Deploy business-class firewalls.
- Secure all wireless networks.
- Implement Internet usage policies that preclude certain personal use.
- Prohibit unauthorized file-sharing programs.
- Deploy proven anti-virus applications and update them regularly.
- Perform regular security audits and correct all deficiencies.

5. Poor backup strategies

It seems that almost every firm wrestles with the issue of data backups. Despite numerous methods and options, many fail to adequately back up their data. Generally, this isn't because the firms don't recognize the need to archive and secure important business and client data. However, confusion and mistakes arise in the details—who, what, when, where, and how.

Fortunately, firms can follow these simple steps to securely protect their data:

- Determine which information is critical to your business and ensure those files are being backed up.
- Test your backup system regularly to confirm it is working properly.
- Work with a proficient technology partner to automate the backup process for onsite and cloud storage.
- Confirm that your cloud backup solution is secure and meets your state bar association's requirements. Generally, you must perform an inquiry of your cloud solution provider. *Michigan has not yet provided an official opinion on the matter.*
- Request confirmations when backups occur and alerts if problems arise.

6. Virus, malware, and spyware exposure

Viruses, malware, and spyware are major threats, and the number and variety of threats are increasing. Nevertheless, firms frequently fail to implement full security suites.

Many law practices self-install anti-virus programs on their systems. However, I often find the installations are inconsistent and

not regularly updated. Even more at risk are firms with no anti-virus applications. Conversely, some may implement an anti-virus solution that is too strong or deployed improperly, crippling network speed.

No virus or spyware strategy is foolproof, but it's recommended that you at least take the following steps:

- Ensure that your operating system is current and security updates are installed.
- Install reputable anti-virus and anti-spyware applications on all servers and workstations with access to the network.
- Regularly update anti-virus and anti-spyware programs.
- Do not let anti-virus and anti-spyware program licenses expire.
- Perform regular automated anti-virus and anti-spyware scans.
- Review security program log files to confirm proper operation.
- Avoid free security products. These products are often deployed in violation of the license agreements and don't support frequent updates, real-time protection, or automated scans.
- Avoid websites known to encourage malicious software.

7. Reliable e-mail

E-mail is a critical communication tool for any law practice. Employing an affordable, easy-to-use, and reliable e-mail solution is essential, yet firms often struggle with their e-mail systems.

Generally, firms experience complications with e-mail because of service downtime, the inability to synchronize with calendars and other applications, no spam filter, and lack of an easy-to-use interface. In most cases, these problems arise when firms use free e-mail services or manage their own e-mail server. Either way, the issues that arise can usually be alleviated with a hosted e-mail solution such as Microsoft Office 365 and assistance from a technology provider.

Here are some functions you should look for when deciding on an e-mail solution:

- Spam filtering
- Size of attachments (you should be able to send files 50GB in size or larger)
- Storage size and archiving
- A service-level agreement guaranteeing at least 99 percent uptime
- E-mail that allows you to collaborate and sync your calendars
- E-mail that is available on all your devices, anytime and anywhere

Conclusion

Simply put, continuing to make the mistakes identified in this article can result in unnecessary expenses, unpredictability, inefficient use of time, and security risks. For an industry that is hyperfocused on client confidentiality and effectively using time, continuing to make these mistakes is unacceptable. An experienced IT provider that is familiar with the needs of law firms will be able to provide you with solutions to these common technology mistakes. And that takes us back to number one on our list—start working with a competent IT provider who understands how you operate. ■

Matt LaMaster is the business development director and corporate counsel for Advantage Technologies, a company committed to delivering IT services to law firms. He is an attorney licensed to practice in Michigan and Florida. He is also a certified Microsoft facilitator and a member of the Microsoft Partner Engagement Board. He can be reached at matt.lamaster@adv-tech.com or (877) 723-8832, ext. 560.

ENDNOTE

1. Telephone conversation with Barron Henley, partner, Affinity Consulting Group (November 11, 2014).