LTT LAW TECHNOLOGY TODAY

July 28, 2016

TEN TECHNOLOGY MISTAKES LAWYERS MAKE EVERY DAY

BY JOE KELLY

An email arrives from an address you don't recognize with an attachment that is marked "important." Since it may be something urgent from a current or prospective client, you decide to open it. However, with a quick click, you could inadvertently download a virus that could hijack every file on your firm's server.

Security is just one of the technology challenges that law firms face every day, and the threats are constantly evolving. Nearly 60% of the respondents to the International Legal Technology Association 2015 Legal Technology Purchasing Survey listed security management as their top IT challenge. That was followed by email management at 48%, information governance at 40% and risk management/ compliance 33%. BYOD, cloud-related security risks and change management were all tied at 22%.

Additionally, Bloomberg reported last year that at least 80 of the largest U.S. firms by revenue have been hacked since 2011.

Lawyers need to understand how even simple errors can compromise their firms, their clients and even their livelihoods. By educating attorneys and staff alike, law firms can keep their data—and their reputations—intact and avoid the top-10 mistakes that occur at firms every day.

Clicking On Attachments From Unknown Senders

While attorneys strive to be responsive, being too quick to open every email can lead to serious consequences. This is the most common way law firms find themselves infected with viruses such as Cryptolocker. According to a report by the Wall Street Journal, more hackers will use malware to hold organizations' data hostage in 2016 than in 2015—and there were more than 4 million samples of ransom-ware in the second quarter of 2015 alone.

Prior to opening an email, check the email address to find out if you recognize the sender and if it is his or her correct information. Also check the subject line and body to help identify any red flags such as typos, inconsistent information or requests for access to personal or financial data. Most importantly, be sure you have robust virus protection installed that can scan attachments and warn you before you hit open.

Storing Unencrypted Client Data On A Laptop Or Mobile Device

Laptops, tablets and phones are prime targets for thieves. They contain almost anything a thief needs to harm your practice–client files, financial information, passwords and personal data. Thieves can auction off the information, use it themselves or can simply sell the device–putting your firm at risk from other unauthorized individuals.

The portable nature of laptops and mobile devices means that they are often in areas that are at a high-risk of theft–cars, restaurants, hotel rooms or subways–when compared to office-bound PCs.

In short, laptops and mobile devices are easy targets. You should avoid storing information on these devices. Instead, opt to store information in the cloud, which offers an elevated level of security including two-factor authentication, intrusion detection systems and encryption. That way, if your laptop or mobile device is stolen, they may have the hardware but not the data.

Failing To Invest In High-Quality Internet

When a new DSL provider offers a cheaper rate for internet access, it may be tempting to sign up. Cheaper isn't always better. That is especially true now that so much data is moving to the cloud. Good quality bandwidth, such as fiber through an internet provider, will always pay off when it comes to staff productivity by eliminating connectivity issues with apps, voice calls and more.

Investing In New Systems Without Considering Security

Clients expect you to provide stellar, seamless service. But they also demand that their data stays secure every step of the way. If your systems do not include top-notch security features, the odds are high that your firm will have to rip it out and start all over again.

This can be a challenge for most lawyers, as security standards and threats are constantly evolving. For example, imagine that you implement an online solution that uses an out-of-the-box firewall. When one of your clients conducts an audit and discovers how basic your security is, they may demand that you install a new software program with enhanced security that includes intrusion detection systems, full-disc encryption and two-factor authentication.

If they do not have a security expert on staff, law firms should consider partnering with a business or consultant that specializes in protecting electronic systems and information. These experts, who are dedicated to staying abreast of technology and its threats, can ensure the highest level of protection for your operations.

Listening To “Bob From Microsoft”

Lawyers are now well aware of cyber threats and are exploring proactive ways to protect themselves. Hackers are now taking advantage of that.

The con starts with this: Someone from a tech support company may call your direct line claiming to have noticed a virus on your computer. When he or she offers to do a screen connect to fix it, you accept their help. But allowing an unverified technologist to remote into your computer is a huge mistake.

No one is ever going to call you out of the blue to fix your computer, no matter how knowledgeable they sound. If you do not recognize the person or the company, you shouldn’t let them anywhere near your computer.

Falling Prey To Proprietary Data Storage

There are hundreds of legal software applications to help you manage your firm. Sometimes trouble arises when law firms outgrow their current software and need to upgrade to an entirely new system. Different software applications format data differently (and oftentimes they have a proprietary format for doing this), which makes extracting or transferring that data out or to another program difficult.

Skimping On Training

At a time when technology plays such a large role in the success of law firms, cutting back on training to save a few dollars can cause extensive harm. Chances are that if a lawyer or a staff member doesn’t understand how programs or apps work, they will either resist using it or won’t be able to take full advantage of all of its features.

It’s like giving someone who has never driven the keys to a race car.

Take the time to fully acquaint all lawyers and staff with new solutions. Have trainers or providers explain how the solutions work, what they offer and how to leverage them in day-to-day tasks.

Handling Your Own Tech Challenges

While some attorneys shy away from technology, others embrace it. You may think you can hire one-off vendors to manage your technology infrastructure and services, but that is usually a short-sighted approach. In the long term, you will probably lose time and money and heighten your security risks. Just think of the lost billable hours, headaches and frustration that happen when you have to call your managed support provider (MSP), explain your tech troubles, and manage their timeline and budget. Choosing the right IT provider that specializes in law firms, cyber security and legal software can make

all the difference. When you hand off IT to the true experts, they can handle your technology issues easily and correctly the first time.

Choosing Solutions Based On Cost, Not Effectiveness

The cheapest solution is not always the one that pays off. Your firm needs to take the time to understand the features of new technology and how your attorneys and staff will use it. Only then can you thoroughly weigh the pros and cons of each new tool. For example, many firms use non-legal-specific software for bookkeeping. It may be cheap, but a good billing and accounting software program designed for law firms is a better choice since it can accommodate specific issues firms face when tracking timekeepers' hours.

Not Taking A Holistic Approach To Technology

When selecting different technology tools and systems, you must consider the needs of everyone, including attorneys, staff and clients. Only then can you select tools that will help meet everyone's goals. That means you, or any other individual attorney, may not be the best person to make decisions on new software purchases.

You should work with experts who are familiar with many different types of software and know how to line up a firm's needs and goals. Experts can bring a completely different, and more encompassing, point of view to the technology selection process as well as a keen eye for helpful and powerful integrations.

In today's world, it's impossible to avoid incorporating technology throughout the practice. Clients won't accept that approach, and younger attorneys wouldn't want to. By avoiding a few common mistakes, you can make technology work to your advantage, not let it hamper or harm your practice.

Joe Kelly, founder and CEO of Legal Workspace, formally launched the company in 2010. In 2006, he first saw the potential for the Legal Workspace solution because of his broad exposure to how law firms operate. The evolution of virtualization, connectivity and hosting technologies made Legal Workspace a commercially viable solution, and it went live with its first client firm in 2008.

Originally published July 28, 2016 by ABA Law Technology Today