Protecting the Kingdom from Technological Disasters

Horseshoe Nails for the Modern Litigator

JEAN-MARIE CRAHAN

The author is with Gonzalez Law LLC, Milwaukee.

For want of a nail the shoe was lost.
For want of a shoe the horse was lost.
For want of a horse the rider was lost.
For want of a rider the message was lost.
For want of a message the battle was lost.
For want of a battle the kingdom was lost.
And all for want of a horseshoe nail.

This tale, handed down with many variations over the centuries, teaches us that seemingly small acts or omissions can have devastating consequences. As lawyers, we research, analyze, and develop solutions to help keep our clients from losing their kingdoms for want of a nail. Sometimes we forget, however, that our own kingdoms—our careers, employees, and clients—can be lost for the want of a nail. Nowhere is this truer for lawyers than in the realm of technology.

Technology advances at warp speed as we continue to counsel, advise, and litigate on behalf of our clients. Every day we witness the power that technology gives us to create. It gives us new, exciting, and efficient methods to accomplish our work. It gives us the ability to communicate and collaborate instantly with colleagues and clients around the world, to learn from the comfort of our living rooms, and to file documents instantly by pushing a button. We can use our computing power in our car, at the airport, in restaurants, or at the beach.

Harnessing the power of technology, we practice our profession. We address old familiar issues and we attend to new and unfamiliar ones. As always, attending to the needs of our clients seems to leave no room for anything else. However, unless we relish the feeling in the pit of our stomachs that occurs when we learn a deadline is missed or that privileged information has been made public or that we've lost all access to our firm information and client files, we must take the time to analyze and mitigate our technology risk. Indeed, our license to practice is at stake. According to the American Bar Association's Model Rule of Professional Conduct 1.1, lawyers are expected to "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."

As with everything else, there is no one-size-fits-all solution to technology risk mitigation. Each lawyer must assess specifically the risks technology may pose to that lawyer's practice and develop redundancies and safeguards applicable to the situation. Universal, however, is the angst we feel when in hindsight we learn that but for a simple nail, saved for times of trouble, we could have saved our kingdom.

Illustration by Max Licht

Published in *Litigation,* Volume 44, Number 4, Summer 2018.

Below are suggestions for technology-related nails that lawyers can lay by to prevent losing the kingdom for want of a nail.

Use Off-Site Data Storage and Backup

Losing access to electronic data on any device or system should not cripple a practice if it is properly prepared. Various scenarios can cause loss of access, including malware, theft or loss, and natural disasters.

Ransomware, virus, or other malware. Computer viruses and malware can wreak havoc on a law firm. Not only can these malicious pieces of code destroy data, but they can also be used to steal proprietary, sensitive, and confidential information. In addition, they can be used to hold a company's data hostage.

On June 5, 2017, global law firm giant DLA Piper published an article online titled "WannaCry ransomware attack was just the tip of the iceberg: 9 things you should know to protect your company from the next attack." The article suggested best practices to defend and respond to ransomware attacks. Ironically, less than three weeks later, DLA Piper itself was brought to a complete standstill when it was hit by a similar ransomware attack. The global cyber event encrypted all of DLA Piper's affected files and requested a ransom paid in bitcoin to restore access or avoid threat of deletion—the demand itself was never quite clear on exactly which.

In the aftermath of the attack, it was reported that firm lawyers were functionally lost with nothing to do, having no access to their work or their emails for days. A firm executive was quoted in the *Wall Street Journal* as saying, "We had planned for the loss of a data center. What we hadn't planned for—and in retrospect it sounds foolish—was the complete loss of everything." This true-life scenario is a perfect example of the "do what I say, not what I do" maxim. While ensuring it gave sage advice to its clients, DLA Piper failed to lay aside the nails it needed to safeguard its own kingdom.

Theft or loss. Computers and other mobile devices are frequently stolen or lost. In 2016, Kensington, a company that supplies desktop and mobile device accessories, surveyed 300 company information technology (IT) professionals to determine the most common places employees experienced theft of IT devices. Cars and other modes of transportation occupied the number one spot. Coming in at second was the office. In one egregious case, a Palo Alto, California, law firm employee stole over 200 firm computers and sold them. Airports and hotels rounded out the top locations for IT theft.

Just as likely as theft, however, is the simple loss of a device. In a 2012 study of seven major airports, it was determined that at just those seven airports, in a one-year period, people left behind 8,016 laptops, smartphones, tablets, and USB devices. The most common places the devices were left? Security checkpoints and restrooms.

Natural disasters. Hurricanes, tornadoes, wildfires, and other natural disasters can cause us to lose access to our electronic information. In 2017, hurricanes Harvey, Irma, and Maria destroyed homes and businesses, including many law firms. In response to the devastating 2017 California wildfires, the California bar's website devoted a page to tips for attorneys on preparing for disaster under the heading "Regulatory Information for Attorneys Impacted by the California Fires."

Regardless of the way in which access to data on a device or system is lost, there is a simple way to ensure that we can keep working through these uncomfortable occurrences. Back up the data in another location off site or in cloud programs that are accessible from any computer that has online access. DLA Piper's downtime after the cyber attack in 2017 may have been minimized had the firm used off-site data storage, cloud-based or otherwise, that was not tied to its network.

When data are backed up elsewhere, losing access to the data on one or more devices will not bring a practice to a screeching halt. Lost data can be recovered by simply downloading the backup to a new computer. This simple solution (an extra nail, if you will) ensures that a practice will not be destroyed by one of these loss scenarios.

Undertake Education and Training for Basic Technological Competence

Just as a farrier knows the type of nail necessary and how to affix it to shoe a horse but doesn't necessarily know how the nail and horseshoe are manufactured, we as lawyers do not need to be able to code to practice competently. Still, we must know how to use the technology tools we do have to accomplish our work. As countless as the programs and devices lawyers use daily to practice are the mistakes lawyers make in their use because they fail to educate themselves on the proper workings of those devices or programs. As the anecdotes set forth below demonstrate, fumbling around with unfamiliar programs can lead to breaches of data confidentiality, missed deadlines, and lost business.

The potential for missed deadlines looms large when one is working with unfamiliar programs. One partner I know went from a law firm with a Microsoft Exchange Server email platform that was accessed through Outlook to a firm that had a dedicated business Gmail account. Unbeknownst to her, the default setting on the Gmail account, unlike her previous account, linked all emails in a chain to one hyperlink in her inbox. She didn't realize that she needed to scroll down to the bottom of each email for the latest information in that chain until after missing several e-filing notifications and emails from clients and opposing counsel. Thankfully, she was alerted to the problem without having suffered any significant adverse consequences.

Disclosure of privileged and confidential information is another significant risk when working with unfamiliar technology. In one hotly contested piece of litigation I handled, in response to my discovery request for certain relevant emails in native format, opposing counsel produced the entire .pst file from his client's laptop. The .pst file is a personal storage table used to store messages, contacts, appointments, tasks, notes, and journal entries from Microsoft Outlook. Not only did opposing counsel demonstrate his technological incompetence in producing this file, but he also disclosed a mountain of his client's confidential information that had nothing to do with the litigation, along with privileged attorney-client emails.

Other more prominent gaffes resulting in the disclosure of confidential information have occurred because lawyers were unfamiliar with redaction technology. In the high-profile baseball steroids investigation, federal prosecutors used a crude portable document format (PDF) blackout technique to redact PDF documents that were then produced. The sensitive information prosecutors tried to keep confidential, however, was made public when a reporter discovered that he could read the "redacted" information by simply cutting and pasting the blacked-out sections of the PDF document into a Microsoft Word document. Because these sections were not redacted properly, the sections showed up as normal text in the Word document and the reporter was able to easily read the "redacted" information.

Resources available to help us get redaction right include the National Security Agency's primer on secure redaction. Nat'l Sec. Agency, Redacting with Confidence: How to Safely Publish Sanitized Reports Converted from Word to PDF (Dec. 13, 2005), www.ca7.uscourts.gov/forms/nsa-redact.pdf. A redaction can be tested by cutting and pasting the redacted content into another document. If the document was properly redacted, no text should be transferred. This test should catch most redaction failures.

Lawyers also need to be aware that competency in legal technology can make or break their efforts to retain existing clients and win new clients. A few years ago, in-house counsel at Kia Motors developed a basic technology competency audit that it administered to its outside law firms. Mock assignments were developed, including formatting a motion in Word, preparing motion exhibits as PDFs, and creating an arbitration exhibit index in Excel. As of July 2013, the test had been administered to, and failed by, nine firms.

The above examples highlight the need for lawyers to understand the use of technology and its limitations. Any lawyer unfamiliar with the technology he or she uses must seek out education and training opportunities to correct the deficiency. It is not difficult to find materials to bring us up to speed. Most software has accompanying user manuals. Read them. Free and paid instruction can be found all over the Internet from sources such as bar associations, private vendors, and educational institutions. Find and take the instruction. Books are written by the truckload to make the more popular software programs accessible to "dummies." Buy them or check them out from a library. In sum, it is our responsibility to ensure that we properly use technology to provide our clients with competent and efficient representation.

Implement Reasonable Security Measures to Safeguard Data

As lawyers, we retain voluminous treasure troves of confidential client information on our IT devices. It is our ethical responsibility to protect this information from disclosure. In addition, we store sensitive information about our own practices on our devices. Everything from firm finances to employee personnel information is stored on computers. While electronic storage is convenient, it also carries significant risks.

Headlines occur weekly alerting us to major data breaches. It is easy to despair when we read that even the global giants, such as Yahoo! and Equifax, fail to protect their information from hacks. Generally lost in the headlines of a data breach, however, is the fact that these data breaches often occur because the simple "nails" weren't laid by; or, if they were, someone either chose not to or forgot to use them.

The following is a non-exhaustive list of security tools readily available and accessible to all lawyers, from the solo practitioner to the employee of a mega-firm, to lessen the risk of a data breach.

Mobile device tools. As described above, mobile device theft and loss carry significant risks of data loss or compromise. Laptop locks assist in thwarting theft and are relatively inexpensive. Software that permits the remote wiping of a device is invaluable in the event such a device is lost or stolen. Encryption software is another tool readily available to protect mobile data. Other options and reasonable security measures should be explored to protect the sensitive data carried around on mobile devices.

Implementation and enforcement of password protection. All devices that store sensitive and confidential information, including smartphones, tablets, and laptops, should be protected with a strong password. It is generally recommended that passwords be 12 to 16 characters long and include characters, numbers, and letters to be secure against brute force hacking attacks. Further, instead of a single word, passwords should ideally be pass-phrases that also include characters, numbers, and letters. Creativity is required to invent a password that is unique, strong, and memorable. After all, a strong password is not useful if the user forgets it. The name of a favorite childhood book, travel location, or song can serve as the basis for a strong, memorable password.

Once a password has been selected, it is necessary to protect its secrecy. Do not store passwords on sticky notes attached to your devices or in your desk drawers or wallets. Refrain from participating in social media quizzes or surveys circulated by friends and family that may reveal potential passwords to bad actors.

Use different passwords for different accounts. Once a cyber criminal learns the password to access one account, that criminal will attempt using that password to access all other accounts of which he or she is aware. Don't let one password fail lead to the compromise of more than one account.

Multifactor authentication. In accounts where particularly sensitive information may be stored, consider using multifactor authentication for access. Access to my firm email account, for instance, requires two-factor authentication. To access the email account, I must first enter my password. Once I have correctly entered the password, the email provider texts a unique randomly generated code to my cell phone. Only after I enter the code from my cell phone am I provided access to my email account.

Develop Policies, Protocols, and Training to Thwart Social Engineering Attacks

"Social engineering" is a phrase used to describe the pretextual efforts by a stranger to gain another person's unwarranted trust. In the context of electronic data, that trust is then exploited to obtain access to computer networks where sensitive information can be stolen, destroyed, or held hostage. Social engineers prey on human psychology—people's natural curiosity and their desire to be helpful or appear agreeable—to compromise their victims.

One common social engineering tactic is to drop infected USB devices in locations where curious employees will pick them up and plug them into their computers. All the firewalls in the world won't protect against a data breach that occurs from inside the network when, for instance, an employee installs an infected USB device on an office computer.

Most USB devices, given their small size, have no labels indicating their content. Unless employees have been trained and tested on the risks inherent in plugging unknown devices into computers, it is highly likely that curiosity will cause them to plug the device in simply to determine what, if anything, is on it.

Other USB devices do have labels or custom inscriptions. Consider what a person might do after coming across a thumb drive with the inscription "Confidential Company Salary Information." Even a person who would not plug in an unlabeled thumb drive might be tempted to plug one in to learn the salaries of his or her bosses and coworkers. Or who could blame the good Samaritan who inserts a red USB drive labeled "Emergency Medical Information" or "Critical Medical Treatment Information," hoping to identify its owner to return it? Custom-inscribed USB drives are readily available for purchase online. I have purchased such thumb drives to use for cybersecurity training. If I can do it, so can the criminals whose job it is to steal, destroy, or otherwise compromise your electronic information.

Criminals know and rely on the fact that people's curiosity or desire to be helpful often overrides the long-forgotten employee handbook directive that inserting unfamiliar thumb drives into company computers is a no-no. To counteract this natural psychology, ongoing, systematic efforts to raise awareness and remind employees of the dangers attendant to such devices are necessary.

Another common social engineering tactic is the phishing email. Phishing is an attempt to obtain personal or sensitive information through email or text by disguising the identity of the sender as a trustworthy person or entity. The tactic may require the email recipients to click on a link that routes them to a fake website that appears to be legitimate. Upon reaching the website, the recipient is then asked to input private information that could give the criminal access to otherwise protected accounts. In other cases, the tactic calls for the email recipient to open an attachment to the email, which then serves as the delivery method for ransomware or other malware.

Many lawyers wrongly believe they will easily recognize phishing attacks and won't fall victim to them. This false sense of security comes from the dated news that cyber criminals have notoriously bad spelling and pose as Nigerian citizens or princes to obtain this information. While amateur phishing scams may continue to include such telltale signs, the lucrative nature of phishing and the related damages it causes have resulted in increasingly sophisticated phishing attacks by well-organized criminals that are not so easily spotted. As with awareness concerning USB device risks, continual efforts to raise awareness and follow-up testing are key to preventing people from being hooked by phishing attacks.

One major company with worldwide insurance, investing, banking, and other financial services conducts extensive training to help its employees resist phishing attacks. It then follows up its training with "test" emails to determine what kinds of emails its employees might fall for despite the training. One relatively recent mock phishing email test circulated by the company demonstrated a high likelihood of success if the email appeared to come from the company itself. The phishing test email had about a 90 percent click rate. The draw? A promotion appearing to be sponsored by the company that would enable employees to win free tickets to a local professional sporting event. This test revealed that although employees might have been on high alert had the email appeared to come from someone outside the organization, further efforts were needed to make them aware of and resistant to phishing attempts that appear to come from inside the organization.

Remember, all it takes is one click to a compromised attachment or link by any employee, up to and including the chief executive officer, to endanger data. To avoid these attacks, don't open emails or click on attachments in emails from unfamiliar or familiar but unverified sources. Also, don't click on links that lead you to enter sensitive information into an unverified website. Always keep in mind the age-old maxim that if it sounds too good to be true, it likely is.

Infected USB drives and phishing emails are only two examples of social engineering tactics. Others include pretexting—where an attacker creates a fabricated scenario to gain unauthorized access. Pretexting might involve an attacker impersonating an external IT services auditor to manipulate a company's staff into providing access into the building. Or the attacker may impersonate company IT personnel over the phone, promising to remotely install software updates that call for the end user to disable anti-virus software. An unsuspecting, untrained employee may gladly hand over the keys to the kingdom in such a scenario.

Piggybacking is another social engineering technique, which involves someone who lacks proper authentication following an employee into a restricted area. If you have ever entered a door requiring card access and held it open for a pizza delivery driver, a UPS driver, or a struggling neighbor, visitor, or other stranger, you are susceptible to piggybacking.

To thwart social engineering efforts, people first need to be made aware of the phenomenon. In addition, there need to be policies and procedures in place that cut down on the risk, such as a "one card swipe, one person" access to a location. Finally, people need to be trained to recognize these efforts and be provided with the tools and support to combat their natural curiosity or instinct to be helpful when the security of data is at stake.

Use Checks and Balances

Most lawyers, but especially litigators, live in a world of deadlines. Missed deadlines can lead to claims of malpractice. It is no wonder that the prospect of a missed deadline causes many of us to lose sleep at night. Technology gives us wonderful tools to lessen the risk of missed deadlines. We can use electronic calendars and reminders to keep track of these deadlines. Our ability to maintain and meet these deadlines, however, is only as good as the information we receive, input, and protect.

To calendar a deadline, one must know the deadline exists. With the increasing prevalence of electronic filing, it is quite common for these deadlines to be communicated in court notices sent via email. Deadlines can be missed because emails containing them are accidentally deleted or misdirected to a spam folder.

In one reported case, a law firm missed an appeal deadline because the notice of the court order that started the running of the deadline went to and was automatically deleted from the firm's spam filter. The firm's plea to the court to excuse the missed deadline fell on deaf ears. The primary basis for the court's decision that the missed deadline was not excusable was the firm's decision, contrary to the recommendation of its IT professional, to save some money by purchasing spam filtering software that allowed the emails directed to the spam folder to be deleted without human review. The lesson here is not to skimp on your email filtering software. Cheap and easy are not the sole adjectives any firm should aspire to have attributed to the firm's ability to receive and process electronic information.

Even had the firm in the above scenario purchased a more robust, more expensive program, however, it is still conceivable that the important notification could have been waylaid. We've all had emails that disappear into cyberspace. In addition, most of us have had the occasion to panic when we inadvertently checked the delete box on an email we wanted to save. To lessen the risk inherent in the delivery and receipt of this type of electronic information, we must create useful checks and balances.

In the above scenario, the firm could have potentially avoided the issue by simply having an assistant tasked with periodically checking the court's docket to ensure that the firm was aware of each significant case event. To avoid a deadline being missed by one set of eyes due to a wrongly deleted email, have more than one person be the recipient of electronic filing notices. Protect calendared deadlines by ensuring that access to modify the calendar is limited to certain authorized personnel. Consider implementing a backup calendar so that deadlines are accessible and saved in more than one location. Use reminders, tasks, and update features in the calendar so that the first time a pleading deadline is seen is not the day it is due or attendance at a hearing is not missed because the lawyer is in Florida on the date the hearing is taking place in Wisconsin. In addition, just as with email redundancy, input the date on more than one person's calendar.

Technology and the speed at which it changes can be daunting and overwhelming. I remember sitting in a conference room in 2006 listening to a discussion about the complexities of e-discovery and thinking, "I hope this issue will pass me by." As a litigator, I soon recognized that these thoughts were unreasonable. E-discovery would soon become a key component of my practice. Therefore, the best thing I could do was take the plunge and educate myself about it. In so doing, I learned that there were ways in which I could more efficiently assist my clients, secure my information, and embrace new technology as it developed. As the tale that commenced this article teaches us, simple tools can prevent large disasters. Lay by technology nails to prevent losing your legal kingdom for want of a nail. ■