The Computer & Internet Lawyer

Volume 34 ▲ Number 7 ▲ JULY 2017

Ronald L. Johnston, Arnold & Porter, LLP, Editor-in-Chief

Technology and Cybersecurity Policies Help Lawyers Manage Technology (Instead of It Managing Them)

By Sharon D. Nelson, John W. Simek, and Michael C. Maschke

Can lawyers actually manage their technology (instead of it managing them)? Can firms create and enforce policies that provide a secure environment for their users and protect client data, rather than acting like computer usage and security is the "Wild, Wild West," where anything goes?

Buying, implementing, replacing, and securing technology are huge challenges—especially when lawyers have billable work to do. Yet, technology (and the policies that govern its usage) is the most important part of a law firm today—at least after the carbon-based units.

What Are Lawyers Doing Wrong?

Rare is the solo/small firm that does an annual review of its technology. Firms tend not to plan, but rather to buy technology when a new need arises, when a partner demands the latest cool tech toy, or when something breaks. In the information security world, that's called the "Break/Fix" method of (not) managing technology.

For the most part, lawyers don't even have a list of all the equipment they own. They don't know when the warranty expires or when it was placed in service—they may think about this briefly in terms of depreciating capital expenses at tax time, but not in terms of planning to replace technology.

They often listen to a vendor they just happen to run into at a conference or someone who persistently stalks them with a deal that sounds too good to be true (Hint: It is). A lot of decisions are made quickly because lawyers are in such a hurry to get back to practicing law. Understandable, but it often results in poor decisions being made.

Getting Organized

First, let's stress an important point: Technology has a life span. For most computers, laptops, tablets, smartphones, etc., that tends to be about three years. That does *not* mean that the devices will cease to work. It just means that consumers

Sharon D. Nelson is president of Sensei Enterprises, Inc., a legal technology, information security, and digital forensics firm based in Fairfax, VA. **John W. Simek** is vice president of Sensei Enterprises, Inc. **Michael C. Maschke** is the chief executive officer at Sensei Enterprises, Inc.

Wolters Kluwer

tend to replace them that often because performance will deteriorate as more is asked of the devices (specifically when software asks more) and because consumers tend to want/need new features in their technology. You may be able to stretch the lifespan of some equipment, such as servers, printers, multi-function machines, etc. to five years.

Second, let's acknowledge that lawyers are terrible about budgeting. Make yourself a list of all the equipment you own, when it was placed in service and who has the devices (this will need updating each year). For the most part, experts recommend that you plan on refreshing your technology, with the exceptions mentioned above, every three years. That means you need to budget for replacing a third of your technology each year. At the least, budget for replacing a quarter of your technology each year.

The ultimate and often-seen nightmare is a "big bang" purchase of almost all new technology because the old technology is so out-of-date. This is a major hit to the law firm wallet. It is far less painful to replace technology over time.

Don't be cheap in your buying decision, because you'll regret it—lawyers need "business class" machines that can handle a lot of software being used at the same time. As these authors have wryly observed, lawyers have zero patience with slow computing.

Don't be cheap in your buying decision, because you'll regret it—lawyers need "business class" machines that can handle a lot of software being used at the same time.

Hopefully, you have a relationship with a trusted IT consultant. Listen to the consultant when it's time to purchase. Don't just willy-nilly buy things because you think you've found a great deal or because a vendor promises you the moon for a song. Your colleagues can be a good source of validation as well. But you should recognize that there are some things you don't know and find someone who can lend a hand. Remember that Model Rule of Professional Conduct 1.1 now expressly includes being competent with technology. If you are not, find someone who is (and if you find competence, hold it close because it is rare).

Security and Ethics—It's a New World

If you haven't read the changes to Model Rule of Professional Conduct 1.6, including the comments, now is a good moment to make a strong cup of coffee and get to it. With the tsunami of data breaches that we've seen in the past few years, even staid and traditionalist law firms have awakened with a start and are scrambling to shore up their data security.

The No. 1 answer to most basic security questions is "encryption is your friend." Strong encryption has not been broken, even by the National Security Agency (NSA) or Central Intelligence Agency (CIA). Your laptops, computers, tablets, smartphones, and backups should all be encrypted.

Lawyers believe encryption is hard. It used to be, but no longer. You don't need to understand the mathematics behind encryption; you just need to have an information technology (IT) pro get encryption set up. For example, if you need to encrypt email, you can install and use a product such as Mimecast Secure Messaging (which we are seeing more and more in law firms) and encryption is as simple as clicking on a "Send Securely" button from within Outlook. If you want to encrypt an attachment (Word or PDF) just put a strong "open" password on it (simple instructions can be found in "Help")—just don't put the password in the accompanying email. Yes, we've seen that. Good grief.

In all aspects of your tech planning and review, consider security. Want to allow employees to bring their own devices and connect to your network? Bad idea. They may be carrying malware and infect your network. Is BYOD (Bring Your Own Device) cheaper? Not if you have a data breach. We've heard folks argue that mobile device management solves the problem. Maybe, but the price of that management has soared in the past several years. Buying and issuing work devices makes the management of their security far easier—and employees have nothing to say about how you choose to manage them.

If your firm has a wireless network, it also should have a guest network that keeps folks away from your business network—creating two distinct, segmented networks. It should be easy-peasy for your IT consultant to set one up.

To Cloud or Not to Cloud?

Every state that has weighed in on lawyers using the cloud to store data has fundamentally said it is fine, so long as the lawyer is reasonably careful to ensure the security of the data. We still have a lot of hold-outs who are not comfortable with the cloud. Our company was long referred to (with good reason) as "cloud curmudgeons"—but we finally came around to the stark realization that most clouds protect data better than most lawyers.

Still, to return to our "encryption" theme, it is important that you make sure that your confidential data is protected. That means that the data has to be encrypted in transit and at rest. Most importantly, you have to be the one who holds the decryption key. In

the case of the iCloud, Dropbox, OneDrive, Box, and Google Drive, the terms of service make clear that these providers have master decryption keys. This is one reason we like SpiderOak, which is designed so that it has "zero knowledge"—you have the only knowledge of the decryption key. Sure, if someone shows up with legal paperwork, SpiderOak can give them data, but it's fundamentally garbage because it's encrypted with the user's encryption key. Even though it is preferred that you control the encryption key, it may not be practically possible, especially when it comes to cloud-based applications.

Technology Users Run Amok—Law Firm Security Policies and Plans

Employees can be rogues, far more apt to do what they please than what their employers dictate. Sometimes law firms try to control their employees with technology. At this point, some employees will end-run the technology with their own devices or networks. Technology is forever limping far behind the wiles of employees who are determined to do what they want—they are tech anarchists. Policies that have a dose of common sense and are well-explained can often accomplish more than technology. Accompanied by periodic training, monitoring, and (we can't stress this enough) discipline for noncompliance, policies work hand-in-hand with technology to secure your confidential data.

Law firms also need plans. In terms of security, the most important plan is an incident response plan (IRP), which you hope to high heaven you never have to implement. In a modern-day nightmare, what happens if you find out that someone has hacked into your law firm servers? What's the plan, Stan?

Policies and plans are an important part of a comprehensive information security program. Policies and plans should be appropriately scaled to the size of the firm, the sensitivity of the information, and identified threats. We could write a complete book on the policies and plans discussed here, but we are just giving you an overview of the basics—there are a lot of resources available that will give you more specifics. This is a condensed version to get you thinking about whether you should be developing policies and plans you don't have or reviewing those you do have to see if they need updating. Remember, there are many more policies and plans that law firms should have, but these are some that specifically are related to securing your data.

For heaven's sake, train, train, train at least once a year, or preferably more often. No one remembers the fine points of plans and policies without at least annual memory refreshers. At a minimum, technology updates will necessitate minor and sometimes major changes, which will need to be learned.

Electronic Communications and Internet Use Policy

There is a lot that can go into this sort of policy, but you certainly want to forbid downloading applications or other executables without the consent of your IT folks. You want to mention drive-by-downloads of malware and explain how pornography and many other forms of Web sites (screen savers and free utilities are notorious) can get malware onto the network just by visiting the sites. Stress known and trusted sites as the only places to visit. Using a secure and properly configured browser (*e.g.*, Chrome) can help as well.

Phishing is the bane of our time and targeted phishing, as we've mentioned, is the most successful way to get into firms. Explain it in your policy and training and give them clues to look for evidence that an email may be a phishing expedition and that no hyperlinks or attachments should be opened.

If you allow the use of social media sites, you'll need to stress the dangers they present, both in the policy and in your training.

If you are going to make rules, you need to be able to monitor conduct, at least periodically, and to enforce them through retraining or discipline. This is true for all policies, so be prepared to police your policies after they are implemented.

A toothless policy won't work. If you are going to make rules, you need to be able to monitor conduct, at least periodically, and to enforce them through retraining or discipline. This is true for all policies, so be prepared to police your policies after they are implemented.

Social Media Policy

Many law firms do not include their social media policy in their Internet usage policy. They make it separate, perhaps because it is such a pervasive problem with unique characteristics. In the social media world, the kids run the household while the parents are left helplessly wringing their hands.

Forbidding the use of social media doesn't work for most law firms. It not only irks employees, but they ignore the prohibition. If you have technology enforcing the prohibition, they will use their smartphones or

other personal communication devices. Stress that social media often is the source of grief with frequent leakages of confidential data.

By way of contrast, large firms generally embrace social media—though we have heard of a few that prohibit its usage. At one general counsels meeting in New York, we heard the general counsels of Sprint and Coca-Cola happily laud their employees as "social media ninjas." They go out and spread messages on behalf of the companies. Of course, in law firms, we have to be mindful of our ethical rules, but within those rules, one can do a lot of good for the firm. So, follow the KISS principle and keep the policy simple. No obscenities, no discriminatory postings, no angry postings, no confidential information, don't speak on behalf of the firm unless authorized, don't give legal advice, remember that social media lives forever, speak politely to everyone you interact with, proof before you post, and report problems to a supervisor. Think *before* you post.

Document Retention Policy

If only law firms would learn to take out the digital trash. Instead, they tend to move all their data when they do a technology upgrade because storage is so cheap. What is not cheap is searching through all sorts of useless data, either when looking for client documents or in response to a discovery request in a lawsuit.

Moreover, if we don't take out the trash, we end up with a lot of "dark data"—data we don't even know we have. We can't tell you how many times we've seen evidence in a case on a flash drive or hard drive and no one knew it was there. Law firms need to manage all their data, securely destroy it when it is no longer needed (if not under a litigation hold or required to retain it because of compliance with laws and regulations) and not leave it lying fallow somewhere where someone might find and expose it, however inadvertently. These devices are ripe for being stolen and often are unencrypted.

Physical Security Policy

You wouldn't, in the paper world, allow files to be scattered around conference room tables when the office is closed for the night and the cleaners arrived. Likewise, you need a policy that might involve alarm systems, prox cards, biometrics, video surveillance, and the physical security of your server, including a locked room with restricted access—or at least a server in a locked rack.

Secure Password Policy

We still are seeing lots of firms without password policies, which is unforgiveable after all this time. Using passwords alone may be a thing of the past before long, but right now most law firms use them. We know we're not going to be very popular with our recommendations, but here are a few things we suggest:

- Employees must have passwords of 14 or more characters. In 2016, we learned that length is more important than complexity, but many firms still require alphanumeric passwords with special characters. There is a good chance this recommendation will be modified by the latest version of the National Institute of Standards and Technology (NIST) guidelines.

- The new NIST guidelines that are expected to be approved by the end of summer 2017 do not recommend frequent password changes. Users are suffering from "password fatigue" and tend to use the same password over and over. The NIST guidelines will recommend less frequent password changes and require immediate changing only when it is known that the password may have been exposed in a data breach.

- Firms should suggest the use of passphrases (IclimbedEVEREST2017!) and prohibit storing passwords on computers or on sticky notes (though storing them on an encrypted flash drive or in a password manager where you have the encryption key is permissible). This includes saving passwords in a browser. In fact, you may want to configure browsers to prevent the storage of passwords.

- Employees should not reuse the password elsewhere or share the password.

- Firms should require both a login and screensaver password that is invoked after a period of inactivity.

Most of the above steps can be enforced through technology. A typical Windows Group Policy can assure that the passwords are a certain length, changed frequently, are not repeated at a certain interval, and are properly applied.

It is now imperative that the length of the password be 14 characters or longer, as the length of a password has become more important than the strength due to the exponential time to "brute-force" the password with each additional character. Historically, the time it takes to crack a password is the only true measure of its worth. However, this is only true for "brute-force" attempts. NIST now believes, and we agree, that most compromised credentials result from the exposure of

login data obtained from some other data breach. The "bad guys" merely obtain the passwords from some other data breach and try all of those passwords against multiple systems as most users reuse the same passwords.

BYOD, BYON, and BYOC

Yes, we know it's an alphabet soup. But the truth is that you need to understand the dangers of having employees getting around security by those acronyms above: Bring Your Own Device (which also can be Bring Your Own Disaster), Bring Your Own Network (which also can be Bring Your Own Nightmare), and Bring Your Own Cloud (which also can be Bring Your Own Catastrophe). If you are going to allow these things, you are going to have to manage them by both policy and technology.

Disaster Recovery Plan

By now, most lawyers understand what a disaster recovery plan is.Your server has had a meltdown, your building is engulfed in flames, or your office is under water. Catastrophes take many forms and many of them impact your data security.We would stress that the No. 1 problem in disaster situations is communication. Make sure your plan identifies who is in charge of what and gives alternative ways to communicate with those who have specific job functions. Protecting lives is the first goal, but then restoring business continuity is key. If your confidential data has been impacted (as happened in Katrina and during 9/11) you have to make one component of your business continuity planning ensuring that your sensitive data remains protected.There are so many factors to consider that it boggles the mind. As we learned when we had a fire and had no access to our office for a week, no disaster recovery plan survives first contact with the enemy. After the disaster is over, you will no doubt find that you need to revisit and revise your plan.

Mobile Security Policies

Lawyer mobility has expanded so much in the last 10 years that most of us can now work from anywhere and have access to our office documents as long as we have an Internet connection. But all this connectivity means we have serious security concerns as we connect with laptops, tablets, and smartphones—not to mention the networks that many lawyers connect to when we are on the road.

If you are traveling, say to China, you might want to take special precautions. A lot of large firms send lawyers with "clean laptops,""throw-away cell phones," and "clean flash drives" so that no confidential data travels to China with the lawyer. It is critical that our remote connections are secure and that we transport and store confidential data in a secure manner.

Equipment Disposal Policy

It can't leave "home" with data on it. So you can't junk your devices or donate them to charity without doing a secure wipe of the data. We recommend a free product called Darik's Boot and Nuke (DBAN), although it will not work on solid state drives. Just make sure you have a policy explaining what must be done and it should be on a checklist for equipment disposal just so you don't forget.

Incident Response Plans

The core of the response function is advance planning. This means attorneys and law firms need a plan, usually called an Incident Response Plan (IRP), which often is focused on data breaches, but "incidents" can refer to responding to ransomware, fighting attempted hacks, combating an insider accessing data without authorization or dealing with a lost or stolen laptop or mobile device.

Most large firms now have these plans in place, but many smaller firms do not. More and more, clients and insurance companies are asking to review law firms' IRPs. In the face of ever-escalating data breaches, now is a good time to develop and implement a plan or to update an existing one.After all, football teams don't get the playbook on game day.

Don't rely on a template IRP. An IRP must be customized to fit the firm—the smaller the firm, the shorter the plan is likely to be.

The problem with all plans is that they may not survive first contact with the enemy.That's OK. Far worse is having no plan at all and reacting in panic with no structure to guide your actions.The first hour that a security consultant or a law enforcement agent spends with a business or law firm after a data breach has been discovered is a very unpleasant time. Kevin Mandia, the founder of Mandiant, a leading security firm owned by FireEye, has called it "the upchuck hour." Not a happy time, indeed.

Don't rely on a template IRP. Although templates may be a starting point, no two law firms are identical and all have different business processes, network infrastructures, and types of data. An IRP must be customized to fit the firm—the smaller the firm, the shorter the plan is likely to be. For a solo practice, it may just be a series of checklists, with whom to call for what.

Books and standards have been written about IRPs. They can be reviewed and qualified professionals can be consulted for more details. The following is a condensed and, hopefully, digestible overview:

The Elements of an IRP

- Identify the *internal personnel* responsible for each of the functions listed in the IRP. Identify them by position titles rather than by name, because people come and go. It will require a broad-based team for a firm of any size—management, IT, information security, human resources, compliance, marketing, etc. Have a conference call bridge line identified in case a breach happens at night or on a weekend and include home/cell phone numbers and personal as well as work email addresses. This list will need to be updated regularly as people join or leave the firm.

- Identify the contact information for an experienced *data breach lawyer* (sometimes called privacy lawyers)—many large firms now have departments that focus on security and data breach response and some smaller firms have a focus on the area. Don't think you can handle this without an attorney who is experienced in data breaches. Your data breach lawyer (if you selected a good one) will be an invaluable quarterback for your IRP team—and he or she may be able to preserve under attorney/client privilege much of the information related to the breach investigation.

- Identify the location of your *insurance policy* (which should cover data breaches). You need to make sure you are covered before you start and list the insurer's contact information because you are going to need to call your insurer as soon as you are aware of a possible breach.

- Identify the contact information for *law enforcement*—usually your regional Federal Bureau of Investigation (FBI) office—often the first folks called in.

- Identify the contact information for the *digital forensics consultant* you would want to investigate and remediate the cause of the breach. Often, a firm has been breached for seven months or more before the breach is discovered, so it will take time to unravel what went on.

- Include in the IRP steps for *containment and recovery* from a breach. A law firm that has been breached has an increased risk of a subsequent (or continuing) breach—either because the breach has not been fully contained or because the attacker has discovered vulnerabilities that it can exploit in the future.

- Determine the *data that has been compromised* or potentially compromised. You'll want to know if all data that should have been encrypted was indeed encrypted in transmission and in storage. If it was, this may lessen the notification burden. Identify any personally identifiable information (PII) that may have been compromised.

- Identify and preserve *systems logs* for your information systems. If logging functions are not turned on or logs are not retained, start maintaining them before a breach.

- If you have *intrusion detection or data loss prevention* software, logs from them should be preserved and provided to your investigators immediately. If you don't, you may want to think about implementing such software.

- Identify the contact information for *your bank* in case your banking credentials have been compromised.

- Identify the contact information for a good *public relations firm* (optional, but often useful). If you are not required to make the breach public, you may not need one. But if it does go public, you may need to do some quick damage control. Your insurance coverage may provide for this, in which case the insurance company will put you in contact with the appropriate firm.

- Determine how you will handle any *contact with clients and third parties*, remembering that you may wish not to "reveal all" (if notice is not required) and yet need to achieve some level of transparency. Be forewarned that this is a difficult balance. You will feel like the victim of a data breach, but your clients will feel as though you have breached their trust in you. A data breach that becomes public can cause a mass exodus of clients, so work through your notification planning with great care. Be wary of speaking too fast before facts are fully vetted. It is a common mistake to try to limit the damage but actually increase it if the scope of the breach turns out to be far greater or different than first known.

- Determine how you will handle *informing employees* about the incident. How will you ensure that the law firm speaks with one voice and that employees

do not spread information about the breach in person or online? How will your social media cover the breach, if at all?

- If you have a *data breach notification law* in your state (and almost all do), put it right in the plan along with compliance guidelines. You may be required to contact your state Attorney General. These laws vary widely, so be familiar with your own state law. Also, determine whether other states' breach notice laws may apply with respect to the residences of employees or clients, the location of remote offices, etc. Make sure that the relevant data breach regulations are referenced in the plan and attached to it.

- Identify any *impacted data that is covered by other legal obligations* such as the Health Insurance Portability and Accountability Act (HIPAA) or client contractual requirements and comply with notice requirements.

- Conduct *training on the plan*. Make sure that everyone understands the plan and their role under it.

- *Test the plan*. This can range from a quick walk-through of hypothetical incidents to a full tabletop exercise to an actual simulated incident. Include contacts with external resources to make sure that everything is up to date. This will help to make everyone familiar with the plan and to identify areas that should be revised.

- Does the breach require that IT and *information security controls and policies* be updated or changed? Does what you learned from the breach require that the IRP itself be revised? The IRP should mandate at least an annual review even without an incident.

Prepare Now

The new mantra in security is that businesses (including law firms) should prepare for *when* they will suffer a data breach, not for *if* they suffer a breach. This requires security programs that include detection, response, and recovery, along with identification and protection of data and information assets. Successful response requires an effective IRP. Attorneys who are prepared for a breach are more likely to survive and limit damage. Those who are unprepared are likely to spend more money, lose more time, and suffer more client and public relations problems.

Cyberinsurance

Do you know if your firm even has a cyberinsurance policy? Many lawyers have no idea what coverage their firms maintain. We regularly hear lawyers insist that their comprehensive general liability (CGL) policy will protect them. It almost never does. Almost all insurers have now riddled the CGL with exclusions to push clients into new specialized cybersecurity insurance policies or riders. Cyberinsurance is its own beast, and a law firm without it in this breach-laden world is very foolish.

The Rapid Evolution of Cybersecurity Policies

Cybersecurity insurance policies, first introduced in the 1990s, are now the fastest-growing segment of the insurance industry. Although fewer than 10 percent of companies in the United States purchase cyberinsurance today, the market is expected to grow by double-digit figures from year to year and could reach more than $20 billion in the next decade. No wonder—a study by the Ponemon Institute estimates that more than one billion records of personally identifiable information have been stolen worldwide to date.

A study by the Ponemon Institute estimates that more than one billion records of personally identifiable information have been stolen worldwide to date.

The Myth That "It Can't Happen Here" Has Vanished

It is now widely accepted that most large law firms have been breached, many more than once. Or put another way, there are two kinds of law firms—those that have been breached and those that will be breached. Very simply, data that has value (and is usually sold on the Dark Web) is a magnet for the bad guys.

Why is cyberinsurance such an important part of information security? The plain truth is that information security has no silver bullet. You can never secure your data 100 percent of the time. A determined and sophisticated hacker can overcome your technological defenses.

How Much Does It Cost?

Cyberinsurance is not cheap, so be a savvy shopper. The prices remain all over the map, so make sure your insurance agent looks around. There isn't yet a good model for measuring prices, risks, and how to hedge the risks—hence the crazy variation in prices that are rising steadily, sometimes exponentially, in reaction to the many well-publicized data breaches of the past year.

Some companies still do not offer cyberinsurance, but there are now at least 50. Many have learned that there is gold to be panned in the cyberworld, particularly because almost all states have data breach notifications laws.

Insurance companies are still gathering actuarial data to assist in setting prices, but as we are in the adolescence of cyberinsurance, pricing is volatile. Solo and small firms are on the lower end of the price spectrum, but it still costs roughly $10,000 per $1 million of coverage annually.

Hacking continues to be such a problem that insurers are now in the process of massively increasing cyber premiums. Insurance companies also are raising deductibles—in some cases by incredible amounts.The list of exclusions is growing, too, so make sure you read that list carefully.

To minimize risk, insurance companies are submitting self-audits to prospective cyberinsurance customers. They also are taking harsher measures, sending in assessors to get an onsite overview of a law firm's security risks and the premium may be based on how closely the assessors' consequent recommendations are followed. If you do have a self-audit form to fill out, don't be slipshod and do be candid.Your false, misleading, or vague answers will be used against you if you file aclaim.

Consider being proactive and abiding by the NIST Cybersecurity Framework. The more you can show that you are ahead of the curve in protecting confidential data, the better your negotiating posture with the insurance companies. It might earn you a preferred premium rate, not to mention the overall benefits of good risk management. As previously mentioned, NIST is expected to approve updates to its guidelines by the end of summer 2017. Make sure you review the changes to the recommendations so that you're not falling behind the cybersecurity curve.

Very few things are as expensive as investigating a data breach, notifying everyone affected by the breach, and otherwise complying with legal requirements through notification and the offer of credit monitoring as well as remediating the problem that caused the breach. This often requires a full-scale security assessment followed by major expenditures to follow all of the recommendations.

Use a good insurance broker, preferably one who is experienced in procuring cyberinsurance. It is amazing how few brokers have expertise in this area or know which companies to recommend. There certainly are companies that have a reputation for denying claims by asserting that they fall under exclusion clauses and others that have a reputation for standing by their customers.

What Will a Prospective Insurer Ask You?

This varies widely. But be prepared for many, many questions regarding:

- Your network diagram;
- The kind of data you hold, including credit card data, PII, HIPAA data, classified data, etc.;
- The nature and frequency of cybersecurity training given to employees;
- Compliance with information security standards;
- Frequency of security assessments—are they conducted in-house or by an independent third party?;
- Policies and plans involving cybersecurity;
- Security currently in place, including firewalls, anti-malware software, data loss protection (DLP) hardware/software, intrusion detection systems (IDS) hardware/software;
- Report of any previous data breaches;
- Security termination procedures upon an employee's departure;
- Physical security of the office(s);
- How the backup is engineered (is it impervious to ransomware?);
- Cybersecurity policies related to vendors and other third parties;
- Do you allow BYOD or BYON? If so, how are they managed?;
- Password policies/enforcement; and
- Encryption policies and software/hardware you deploy.

What Coverage Am I Looking For?

There is no consistency between the coverage of the various insurance companies, and they all use different language. It is very hard to determine exactly what you're purchasing, much less make an apples-to-apples comparison.

What if data is somehow transported to a social media site? Are you covered there? How about data breaches in the clouds? It is widely reported that cloud

providers tend to have less coverage than might be prudent from the point of view of the law firm that engaged the cloud. Just read your cloud vendor's terms of service; we can guarantee that the provider will try to insulate itself from liability. With 50 percent or more of law firms storing at least some data in the cloud, this is a threshold question to ask.

Not surprisingly, with all the confusion, battles over coverage have wound up in court. In *Zurich v. American Insurance Co. v. Sony Corp. of America*, Zurich was seeking to absolve itself of any responsibility to defend or indemnify Sony for claims asserted in class actions and other actions stemming from the 2011 hacking of Sony's PlayStation Network. Zurich maintained that the general liability policies it sold to Sony did not apply. Ultimately, the court agreed. If Sony's lawyers didn't know what their insurance covered, imagine the fog a solo or small-firm attorney might be in.

One of the more recent developments is that insurance companies were moving to offer "business interruption" coverage as part of their cyberinsurance policies. This is definitely something you want to inquire about.

Another cyberinsurance mantra to understand is "We Don't Cover Stupid"—referring to an insurance company's refusal to pay a claim when a company that had been breached had not followed "minimum required practices" as spelled out in the policy. This story doesn't involve a law firm but it is instructive for law firms to read it. We've seen a number of insurance companies say there is no coverage when security of confidential data is sloppy.

How Insurers Dodge Liability

Insurers dodge liability in a number of ways, including:

- Not paying retroactively. Given that breaches can be discovered months after the compromise, law firms should carefully consider when coverage starts.

- Terrorism/act of foreign enemy exclusions. Many cyberattacks originate from outside a country's borders, and many of them are believed to be state-sponsored. Depending on the policy's wording, your firm could be left high and dry.

- Lack of coverage for negligence. Insurers are starting to cover only data theft, not negligence. If an employee loses an unencrypted laptop with sensitive data, some policies won't cover the breach.

- Failure to make a timely notification to the insurance company. Make sure you know when you need to report an incident to your insurer. The clock may be ticking and you don't want to find that your delay means that there are costs you cannot recover—and remember that costs start to mount up quickly after a breach.

In the end, you will have to balance the costs of making security improvements with the cost of cyberinsurance to determine where you are getting the maximum benefit and limiting your risks as much as possible. It is not an easy calculation.

In the end, you will have to balance the costs of making security improvements with the cost of cyberinsurance to determine where you are getting the maximum benefit and limiting your risks as much as possible. It is not an easy calculation.

Cybersecurity Basics

Cybersecurity is a hot topic these days, but what does it mean to practicing lawyers? Essentially, cybersecurity is the protection of your information systems from theft or damage. For an attorney, that means making sure your client's information stays confidential. Today, that includes taking steps to protect yourself from experiencing a data breach.

Are lawyers doing enough to safeguard law firm and client information? Our opinion is that many are not. Here are a few reasons we hold that opinion:

- The FBI reported at a legal technology conference in 2013 that they are seeing hundreds of law firms increasingly being targeted by hackers.

- Mandiant, now part of InfoSec giant FireEye, reported that 7 percent of the breaches it investigated in 2014 involved law firms.

- Another report noted that 80 percent of the largest 100 law firms, by revenue, had been hacked between 2011 and 2015.

- At a meeting of large firm information security experts from Washington, DC, most admitted that they had been breached—and that they were aware from their colleagues that others had been breached as well.

- Even with the dismal record of reporting law firm data breaches, we still learn of them in the press and informally—and we will detail some of them for you.

Although data breaches can happen despite reasonable (or even stronger) security, the frequency of law firm data breaches and reports on how some of them have occurred suggest that many attorneys have not been employing reasonable safeguards. Why do many otherwise competent lawyers fail so miserably in protecting firm and client data? Here are some of the reasons:

- Ignorance—they simply need education and many of them don't know they need it.

- The "it can't happen here" mentality is flatly wrong. Since the FBI issued an advisory in 2009 warning that law firms specifically were being targeted by identity thieves and by those performing business espionage, it has continued to meet with large firms to discuss information security. We were, in earlier days, worried about cybercriminals, China, and other state-sponsored hackers, which continue to be major threats. Thanks to Edward Snowden, we also know that we need to worry about surveillance by our own government.

- According to press reports, lawyers and law firms are considered "soft targets"; they have high-value information that's well organized and frequently have weak security—although we are happy to report that, at least at large firms, cybersecurity is now a pretty high priority.

- Though there are many low-cost/free measures that solo and small-firm lawyers can take to protect sensitive data, true information security, including hardware, software, training, etc., can be expensive. Protecting the security of client data can present a big burden for solos and small law firms. This does not take away a lawyer's ethical duty, however, and it is one reason we lecture so often on computer security. After a lawyer sees the most common vulnerabilities, he or she can take remedial steps—or engage an IT consultant to do those things that are beyond the lawyer's skill.

- The need for vigilance never stops. You cannot secure your data once and think you're finished; the rules of information security change on close to a daily basis. Certainly, someone in the firm needs to keep up with changes regularly or the firm needs to engage a security consultant to do periodic reviews. Although the necessary frequency of security assessments depends on the size of the firm, the sensitivity of the information, and identified threats, it is our judgment that mandatory assessments should be conducted at least annually. Also, clients are beginning to demand self-audits or third-party audits of law firm security. We have never seen a client who passed such an audit on the first go-round. In fact, they don't even understand the audit questions, which doesn't bode well for the results.

Detect and Respond

In a more innocent time, we thought we could keep the barbarians outside the walls that guard our data. Alas, those days are gone. For years, the emphasis was on preventing villains— cybercriminals, state-sponsored agents, business espionage spies, and hackers—out. We went from fairly simple anti-virus software to sophisticated anti-virus software and, finally, to enterprise anti-malware software security suites.

The products got better and better and better. Sadly, what we learned is that all the would-be intruders were not only matching the good guys step for step, they were outpacing them.

It took a surprisingly long time for everyone to "get it," but in the end we realized that if the bad guys are smart enough and target a particular entity, they are going to successfully scale the walls we built to keep them out. With that realization, "detect, respond, and recover" became the new watchwords in cybersecurity.

Mind you, we are still trying to keep the bad guys out; that is our first line of defense. But now that we know that our first line of defense is a Maginot Line for sophisticated attackers, we have moved forward in our thinking.

The NIST Cybersecurity Framework

In February 2014, we took a step toward securing our data and the physical infrastructure protecting it when the National Institute of Standards and Technology released Cybersecurity Framework Version 1.0. The framework provides a structure that organizations, regulators, and customers can use to create, guide, assess, or improve comprehensive cybersecurity programs. This came as a result of Executive Order 12636, issued in February 2013, which called for "the development of a voluntary, risk-based Cybersecurity Framework—a set of existing standards, guidelines and practices to help organizations manage cyber risks. The resulting framework, created through public-private collaboration, provides a common language to address and manage cyber risk in a cost-effective way based on business needs, without placing additional regulatory requirements on businesses."

The framework allows organizations—regardless of size, degree of cyber risk, or cybersecurity

sophistication—to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure.

The document currently is in the process of being updated to version 1.1 with comments currently being reviewed, and provides new details on managing cyber-supply chain risks, clarifies key terms, and introduces measurement methods for cybersecurity, all in the hope of making the document easier to read and use.

Here is where you find the magic words of the document, "identify, protect, detect, respond and recover" that should shape any law firm's cybersecurity program.

"Identify and protect" was where we started in the early days of cybersecurity. Although those words are still important, "detect and respond" have surged forward as a new focus—along with, of course, recovering from security breaches, which is no easy task. It is especially tough if you don't know you've been breached.

What Does "Detect and Respond" Mean for Law Firms?

Detect and respond means rethinking how you approach the security of your data. Now that you know that you can't keep a determined intruder out, you know you need to detect them after they've penetrated your network. So, you need technology and software that will help you detect that you've had what is called, in polite circles,"a cybersecurity event"—translate that to "a breach."

As you can imagine, you want to know of these "events" as soon as possible so you can take action.Today, there are technology solutions that identify "anomalies" in your network (things that are outside the norm) or that look for executables that are unknown but are behaving like malware or some other form of cyberattack.Although some of the solutions may be beyond the need or the budget of solos and very small firms, you don't have to be very large to start considering heading down this road.The risks of not doing so are simply too great. The good news is that there are technical solutions that are very affordable and would be a good starting point for the solo and small-firmattorneys.

Some of the solutions include data loss prevention (DLP) software and appliances, intrusion detection systems (IDS), intrusion prevention systems (IPS), electronic content management systems (ECM) and security event management systems (SEMS). When you meet with someone who can explain the various solutions to you, brew a pot of expresso—you're going to need to be highly focused to understand how one solution differs from another.This is really cutting-edge technology that changes from month to month (if not day to day).

First, we recommend that you start by investigating intrusion detection systems. An intrusion detection system watches network and system activity and alerts you if there appears to be some malicious activity. It begins by creating a baseline of network traffic. Any suspicious activity outside of the configured parameters (*e.g.,* 10 percent additional network bandwidth utilization) causes an alert, which typically is an email message to an administrator. One of our favorite IDS products is Meraki by Cisco. It is subscription-based and only costs a few hundred dollars a year. The hardware itself is under $1,000 dollars and then you only have to deal with annual subscriptions after that. The system is cloud-based and updates are automatically delivered and installed. The updates are based on the activity seen by all the Meraki devices in the Cisco network. In other words, you take advantage of having fixes applied based on malicious activity that someone else may have experienced. Needless to say, Cisco is a very trusted brand.

As for your response to your incident, that may vary. After the initial panic, you will want your in-house or outside technology consultants (and you are likely to need digital forensics technologists, who are more familiar with data breach investigations) to take a look at the situation and see what they can determine. After they understand what has happened, they also can figure out how to "plug the hole" and otherwise mitigate the breach. Remediation of whatever caused the breach is key.

Hopefully, you already have an incident response policy and plan in place, no matter how big or small your firm might be. For all but the smallest firms, there also should be an incident response team in place to implement the plan. At a minimum, you should already have identified who will be involved along with their appropriate roles.

In all probability, you will want to call a lawyer familiar with data breach laws who can advise you on complying with any of the 48 state data breach notification laws. If there is data protected by federal law (such as HIPAA data), you'll need advice on that front, too. Finally, one of the first pieces of advice you are likely to be given is to call the FBI. Although that is anathema to most law firms, it is the appropriate course of action. Remember that the FBI makes no public statements about these investigations and doesn't show up in flak jackets or otherwise make a public display of your "cybersecurity event." You can determine which FBI office to call by performing a Google search for "FBI regional offices" and entering your zip code.

The ABA Cybersecurity Resolution

The American Bar Association (ABA) has weighed in on cybersecurity concerns, always a sign that the

states may follow. On August 12, 2014, the ABA House of Delegates passed, without opposition, a cybersecurity resolution, Resolution 109, which reads as follows:

> RESOLVED, That the American Bar Association encourages private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected.

You might be forgiven for thinking as you read the resolution:Wow, that really says a whole bunch of nothing. And you'd be right—it is really a cautionary resolution intended to raise awareness.

There is a back story to the resolution, which was much larger in its original format. The original resolution appeared to command all law firms, large and small, to come up with a cybersecurity program that met national and international standards.

This met with fierce opposition from a number of ABA entities, including the Law Practice Division and the GP/Solo Division. The resolution was submitted by the ABA Cybersecurity Legal Task Force and the Section of Science & Technology Law.

In answer to the controversy, the language of the resolution (which stands on its own and is not governed by the accompanying report) was watered down to this tepid version. At the behest of other entities, language in the report also was changed to make it clear that the resolution was not attempting to make a change in lawyers' ethical duties and to add language recognizing that smaller firms could not be expected to adopt a program that made no sense considering their size and budget constraints.

Clearly, for small firms, the international and national standards cited in the report appeared fearsome. There are standards for smaller firms such as the NIST standard mentioned previously.

The report states: "Small organizations, including small law firms and solo practitioners, can prioritize key cybersecurity activities and tailor them to address the specific needs that have been identified." For help with this, you might check out NIST Internal Report 7621 Revision 1: *Small Business Information Security: The Fundamentals*. The original report was written in 2009 and was updated to Revision 1 in November 2016. Target hardening is one of the sections. It would seem pretty obvious that you should be beefing up your security in order to reduce the chance of compromise, but most people just set it and forget it.

Cybersecurity Worries

There are lots of cybersecurity worries to give you the willies in the wee hours of the morning. Here are a few of the most common ones we see:

Ransomware

We continue to see law firms struck by ransomware, which encrypts your data followed by a demand for payment—usually in bitcoins—to get your data back. Training your employees not to click on suspicious attachments or links in email will help. They need to stay away from suspicious sites as well, because ransomware can be installed by just "driving by" an infected Web site.

Overwhelmingly, from a technological standpoint, you can defeat ransomware by having a backup that is immune to it.This can mean, particularly for solo lawyers and small firms, that they backup to an external USB drive and then disconnect the backup from the network. If you leave it connected, the ransomware will encrypt your network AND your backup. For others, it means running an agent-based backup system rather than one that uses drive letters or network shares. Make sure your IT consultant has your backup engineered so that backups are protected. That way, even if you are attacked with ransomware, you can thumb your nose at the demands for money because you can restore your system from your backup (which means backups need to be made frequently to avoid any significant data loss. There always should be a good backup that is NOT connected to the network).

Employees

Employees are by nature rogues. In every study that's been done, they will ignore policies (assuming they exist) in order to do what they want to do. This often means they bring their own devices (BYOD), bring their own network (BYON), or bring their own cloud (BYOC). Certainly your policies should disallow these practices (in our judgment) or at least manage the risks by controlling what it is done by a combination of policies and technology.

Targeted Phishing

This is perhaps the greatest and most successful threat to law firm data. Someone has you in their sights.They often have done research on your law firm. They may know what cases you are involved in and who your opponents are.They may know the managing partner's nickname. Everything they know about you they may use to get you to click on something (say, an email from an opponent referencing a specific case and saying "The next hearing in_____case has been rescheduled

as per the attachment.") Many a lawyer has clicked on such attachments or a link within an email.

The best solution to protect yourself from targeted phishing is training—and more training—endlessly. One California firm had multiple target phishing attacks but survived them because attorneys and staff who received such emails questioned their authenticity. Forget the loss of billable time. The loss of money, time, and even clients due to a data breach can be far worse.

Interception of Confidential Information

Start with the proposition that everyone wants your data, including cybercriminals, hackers, and nation states (including our own). Frankly, if they want your data and they have sophisticated tools, they will get it. So shame on you if you are not employing encryption (which is now cheap and easy) to protect confidential data via voice, text, and email. Encryption, today, is a law firm's best friend. You may choose to use it always or in cases when it is warranted—but you surely should have the capability of encrypting.

Failure to Use Technology to Enforce Passwords Policies

First, let us say that you should use multi-factor authentication when available and use it to protect sensitive data. But failing that, we recognize that passwords are still king in solo/small/mid-size firms.

Therefore, have your IT consultant assist you in setting up policies that can be enforced by technology, requiring that network passwords be changed on a periodic basis, not reused for an extended period of time and mandating strong passwords of 14 or more characters in length. Passphrases are best. 1lovepracticingl@w2017! would do nicely.

How are you going to remember all of those unique 14+ character passwords? This is where a password manager is your friend. Password managers store the data in an encrypted "vault" that is accessed using a very strong master password. You put all your logon information into the software database where it is stored as encrypted data. Some password managers can store a wide variety of data and not just username and password. Some automatically will fill in the login information without you typing a thing. Some can store additional information such as credit card numbers, passport information, prescriptions, frequent flyer numbers, and any other desired information. Finally, when selecting a password manager, you'll need to decide if you want the encrypted password vault to be stored in the cloud or locally on your device. Either one is acceptable because the data is encrypted with a password you define.

Securing Your Equipment—What To Do

Computers and mobile phones are the workhorses for virtually all attorneys today, although there has been some movement to tablets as "PC replacements." Windows is the dominant operating system for lawyers, but Apple's OS X has been gaining, particularly in the last few years.

Computers (Desktops, Laptops, Tablets)

The basic steps for securing personal computers, whether at home, in a law office, or on the road are:

1. Use strong passwords, passphrases, or other strong authentication (such as biometrics).
2. Operate in a standard user account without administrator access for routine use.
3. Configure the operating system, Internet browser, and other software in a secure manner.
4. Install and use security software, including malware protection and a software firewall—and keep them current with updates.
5. As patches (software fixes) are released, apply them to the operating system and all programs and applications, including browser plugins.
6. Install and use a hardware firewall for the local network.
7. Enable full disk encryption on laptops—hardware, in the operating system, or with an encryption program.
8. Backup important files and folders or the complete drive.
9. Use care when downloading and installing programs.
10. Be careful when browsing the Internet.
11. Use care with email attachments and embedded links.

Authentication

Authentication and authorization form the first line of defense for desktops, laptops, and servers. Desktops, laptops, and servers should, at a minimum, be protected with a password or passphrase. Major laptop manufacturers offer fingerprint readers as an option. More advanced authentication and multifactor authentication should

be considered for laptops and servers, particularly for remote access. With the strong support for fingerprint authentication and facial recognition in Windows 10, laptops with hardware to support these authentication methods are likely to become more common.

With the strong support for fingerprint authentication and facial recognition in Windows 10, laptops with hardware to support these authentication methods are likely to become more common.

User Accounts

Both Windows and OS X have multiple kinds of accounts for users. They include standard user accounts and administrator accounts. The standard user accounts have limited privileges. Administrator accounts have more privileges and can, accordingly, do more, such as installing new software and devices. For routine use, computers should be operated in standard user account mode. Administrator accounts should be used only when necessary to perform functions that are limited to them. Operating in a standard user account provides better protection because some (but not all) malware and attacks need administrator access to be successful. When operating in an administrator account, it is particularly important to pay attention to dialogue boxes and warnings.

In Windows, local user accounts are managed in the Control Panel. In OS X, user accounts are managed in System Preferences. In networks, passwords often are managed centrally with tools such as Microsoft's Group Policy in a Windows environment.

Secure Configuration

Secure configuration or "hardening" is the process of setting up or adjusting the operating system, Internet browser, and all applications in ways that maximize security and minimize the potential for compromise. The approach should use the highest security settings that will allow the computer to perform necessary functions. In addition, services and functions that are not necessary should be disabled or blocked.

Current versions of operating systems and application software should be used because they generally are more secure than older versions. For example, the current versions of Windows and OS X have more security functionality than older versions. Microsoft Office 2016, Microsoft's Edge browser, and Adobe Acrobat DC and Reader DC all have much stronger security than older versions. Unless there are compatibility issues with other applications, upgrades should be promptly made.

During installation, the user is prompted for various security settings and enabling of various services. When in doubt, choose the higher security settings and do not enable services that you do not need. For questions, check the installation instructions and help files or consult someone with technical knowledge.

The following services should be disabled if you don't need them: print sharing, file sharing, window sharing, and remote login. They present unnecessary security exposure if they are not being used. If you use them, you will need to enable them and manage the risks. For example, remote login should be set to require strong authentication. Multifactor authentication is best.

The first step is setting up user accounts as discussed earlier. Security software (including a firewall), patching, and browser configuration are all important parts of hardening and will be subsequently discussed.

Although the technical details of secure configurations are beyond the scope of this article, they are available on Microsoft's Web site at *https://www.microsoft.com/en-us/security/default.aspx* (for nontechnical users) and *https://technet.microsoft.com/en-us/security/bb291012* (for technical users). Articles on secure configuration of Windows are available at *https://technet.microsoft.com/en-us/windows/security-and-control.aspx* and *https://technet.microsoft.com/en-us/library/mt601297(v=vs.85).aspx*. Apple has Security Configuration Guides for the various versions of OS X in the Support section of its Web site at *http://www.apple.com/support/security/guides/*. For those with technical ability, there are various tools to assist with secure configuration. Microsoft has tools such as the Microsoft Security Compliance Manager, Microsoft Baseline Security Analyzer (a tool that allows users to scan one or more Windows-based computers for common security misconfigurations) and the Security Configuration Wizard (to assist in creating, editing, applying, or rolling back security policies with Windows Server). NIST has published security configurations for various operating systems and software as part of the US Government Configuration Baseline and the Federal Desktop Core Configuration. Compliance with them generally is required for federal agencies, and they can be used as guidance for others. The Center for Internet Security (CIS) Security Benchmarks Division publishes consensus security configuration standards for operating systems, browsers, servers, network devices, and mobile devices (*https://benchmarks.cisecurity.org*). Automated tools are available to test computers for compliance with these standards, including tools published by CIS.

Another publisher of these kinds of tools is Belarc (*http://www.belarc.com*). Its Belarc Advisor builds a

detailed security profile, including missing Windows patches and security configuration. It only is available as a free download for personal use and not for commercial or government purposes. Belarc does make products for commercial usage such as BelSecure and BelManage. Additional tools are discussed in the subsequent Patching section.

Although there has been much debate about the need for security software on Macs, let it end here. Macs are vulnerable as has been demonstrated many, many times over the years.

Security Software

Security software should be used on all desktops, laptops, and servers. Although there has been much debate about the need for security software on Macs, let it end here. Macs are vulnerable as has been demonstrated many, many times over the years. There is no reason to take a chance in light of the ready availability of security software and its low cost. The malware targeted at Macs is increasing as Apple's market share has grown. In Macs running both OS X and Windows, both operating systems should be protected. In recent years, the major security software vendors have moved from individual products, such as antivirus and firewalls, to security suites that integrate multiple security functionality, such as malware protection, software firewalls, Web browsing protection, and spam filters. Some of them include advanced features such as rootkit protection and basic intrusion protection.We're beginning to see encryption capabilities available as well. They offer the advantage of being a single integrated product, which is easier to install, configure, manage, and keep up to date.

Various publications, such as *SC Magazine*, *CSO*, *PC Magazine*, *CNET* and even *Consumer Reports*, rate security software from time to time. It is a good idea to look at current reviews before selecting a new product. Although opinions vary on which product is best at any given time, it is clear that any of the major security vendors' current security suites, with up-to-date definitions, will make a desktop, laptop, or server significantly more secure than one that is not protected. Some leading vendors include Symantec, McAfee (Intel), F-Secure, Sophos, Trend Micro, and Kaspersky. Vendors are now offering multi-device packages that provide protection for up to three or five devices—desktops, laptops, and smartphones—for both PCs and Macs.A list of security software for Macs can be found at *http://mac-antivirus-software-review.toptenreviews.com*. The authors have had good experience with Kaspersky, F-Secure, Sophos, and Symantec products.

One of the ways that security software detects malware is through the use of signatures. A signature looks for a specific known pattern of code that has been found in the malware. In addition to specific malware signatures, some of the newer security software also reviews more general patterns of behavior to attempt to detect malware for which there are not yet signatures. Some security software for desktops, laptops, and servers also includes basic intrusion protection. Security software that is out of date is only marginally better than no security software at all.

In addition to security suites, there are software host intrusion prevention systems (IPS) that provide a more advanced level of protection to laptops and desktops. They have stronger capability to protect against unknown threats.They generally are centrally administered in networks rather than used as stand-alone solutions on individual computers or in small networks. Some examples are IBM EPP, Symantec Endpoint Protection, and McAfee Host Intrusion Prevention for Desktop. At the network level, host IPS often is used to protect servers.

There is an ongoing arms race between security vendors and malware authors. Signatures are written to detect known malware, and then malware writers change their code to avoid detection. Because of this, it is critical to keep the security software up to date with new definitions, which often are available multiple times a day. Security software generally should be set to automatically receive updates.

A firewall is software or a device that controls the flow of data to or from a computer or network. It helps protect against attacks from the outside. Some firewalls also block or alert to outbound traffic. Both Windows and OS X now include built-in software firewalls. Many consider the firewalls in the security suites to provide better protection than the built-in ones. One or the other definitely should be used. In a law firm, firewalls in security suites generally should be used in addition to a hardware firewall for the entire network.

Patching

A vulnerability is a flaw in software. An exploit is code that takes advantage of a vulnerability to cause unintended or unanticipated behavior in the software. It can range from causing the software to crash to giving an attacker complete control of the computer. Software vendors prepare and distribute patches to address vulnerabilities. Patches frequently address security issues.

It is critical to apply security patches promptly. Until they are applied, a computer is exposed to the

vulnerability. Where available, it generally is best to allow automatic downloads of updates. This feature is available from Microsoft and Apple. One caveat is that, in a network environment, it is sometimes necessary to test patches before they are applied. Although they have been tested for the vendor's products, they may cause problems with other vendors' products, including legal applications such as case management and document assembly products.

With Microsoft products, the patching process is not difficult because Microsoft issues patches each month on "Patch Tuesday," including patches for Windows, Internet Explorer, the Edge browser, and Microsoft Office. Apple issues patches less frequently and OS X can be set for automatic download when they are issued.

The significant challenge is making sure that everything else is patched: applications, media players, browser plug-ins, and on and on. Security studies frequently report that they find exploits that target vulnerabilities for which patches have been available for a long time. One reported that the most commonly blocked attack was for a vulnerability for which a patch was available for months and the second was one for which a patch had been available for almost three years.

A zero day attack, under varying definitions, is one that attempts to exploit a vulnerability not known to the software developer or to the security industry or for which a patch is not yet available. For this reason, they are particularly dangerous. Some of the zero day attacks in the past year have exploited vulnerabilities in Microsoft Windows, Microsoft Office, Apple OS X, Adobe Acrobat and Reader, Adobe Flash, and Java—all programs regularly used by attorneys. Zero day attacks most frequently are used in targeted attacks (against a specific victim or group of victims) but are sometimes used in more widespread attacks.

Installing Programs

It is important to exercise care in selecting and installing programs. In a law firm, only necessary programs should be used. Every installed program increases the surface for potential attack and must be managed and kept up to date.

When downloading programs from the Internet, use only trusted sources and pay attention to warnings about certificates. On the Internet, code signing with certificates verifies the source of the code and shows that it has not been tampered with. If a warning pops up that the certificate is invalid, don't install the program.

Peer-to-peer file sharing should not be used on law firm or business computers. It has the potential to expose all files on the computer and potentially other data on a network.

Safe Browsing

Internet browsers, such as Microsoft Edge (new with Windows 10), Internet Explorer, Chrome, Safari, and Firefox, are great productivity tools for attorneys because they are the gateway to the vast information resources of the Internet and serve as the interface to access cloud resources such as software as a service. Unfortunately, they also are the gateway to the dark side of the Internet where criminals are trying to do nefarious things such as steal information or take over vulnerable computers.

Just visiting a malicious Web site or a compromised legitimate site may be enough to compromise a computer (called drive-by malware). A scary example is that *The New York Times* Web site was reportedly infected through the compromise of a third-party service that fed ads to the site. Just a visit to the site was enough to expose a computer to malware.

Be very careful about visiting Web sites with which you are not familiar. Malicious sites frequently have appeared high in search engine results. Some security products provide warnings about known malicious and suspicious sites.

Fortunately, the security of browsers has improved greatly over the years and today's browsers are more secure than older ones. For this reason, it is important to use the latest version of the browser, to configure it securely, and to stay current with patches.

If the security software or browser provides a warning, pay attention to it. Don't blindly click "OK." Some of the newer browsers include features called sandboxes that isolate the browser from the operating system. They provide warnings if a Web site tries to install a program or to access the operating system. But they can be defeated if a user blindly clicks "OK" and ignores their warnings.

As mentioned previously, routine operation of a computer should be in a standard user account and not an administrator account. This is particularly important when surfing the Web. Secure configuration of the browser also is a key step. In Internet Explorer, this is controlled by clicking on Internet Options, under Tools, and then clicking on Security. It should be set to medium-high or greater. Custom levels also may be set, but this is better left to someone with technical knowledge. Disabling of functions such as ActiveX, Flash, Java, and JavaScript provides greater security but also affects functionality. Do not install or enable browser plug-ins unless you need them. Use current versions and keep them patched.

A vulnerability in a plug-in still leaves you exposed even if the browser itself is up to date. Some businesses are putting the browser in a sandbox that isolates it and helps protect against attacks. If the browser is partitioned off, data elsewhere remains safe.

When you visit a site where you have to enter a username and password or provide any confidential information, make sure that the displayed Web address starts with "https." In Internet Explorer, a picture of a lock also is displayed. The "s" means that it should be a secure connection. It's not an absolutely sure thing, though, because Web sites can be spoofed and you may have a secure connection to a malicious Web site. Use of multifactor authentication and approaches such as the digital certificates used by Windows 10 Passport protect against interception or compromise of usernames and passwords.

Attachments and Embedded Links

Email attachments frequently are used to install malware. Embedded links in emails often are used to take the user to an infected Web site. Don't open attachments from unknown sources and scan attachments for malware before you open them. Be very careful of clicking on links unless you are sure of the sender and are familiar with the site. Phishing (falsified emails purporting to be from banks, PayPal, eBay, and other legitimate sites) is now a very common form of attack. It attempts to steal information, often logon credentials, either by trying to trick people into providing them or by planting malware that steals them. Some malware can be installed by opening an infected attachment or just visiting an infected Web site. The Anti-Phishing Working Group is a helpful source of information (*https://www.apwg.org/*). Attorneys and law firm staff should be trained periodically about this risk.

Encryption

Encryption is becoming more important to protect data on desktops and laptops. Most security professionals consider encryption to be a security no-brainer for laptops and portable devices. Although not commonly used, some law firms also are starting to encrypt desktops and servers—some driven by client requirements.

To avoid the loss of data, it is important to understand how the encryption works, to back up data that is encrypted, and to keep a copy of the recovery key in a secure place. Enterprise controls are available to centrally manage encryption.

Disk Encryption Basics

There are two basic approaches to encrypting data on hard drives: (1) full disk encryption and (2) limited encryption. As its name suggests, full disk encryption protects the entire hard drive. It automatically encrypts everything and provides decrypted access when an authorized user properly logs in. Limited encryption protects only specified files or folders or a part of the drive. With limited encryption, the user has to elect to encrypt the specific data by saving it in an encrypted partition or folder. Because it can be easy to forget to put confidential data in an encrypted partition or file, full disk encryption is usually more secure and therefore recommended.

Most security professionals consider encryption to be a security no-brainer for laptops and portable devices. Although not commonly used, some law firms also are starting to encrypt desktops and servers—some driven by client requirements.

There are three options for protecting laptops and portable devices with encryption: (1) hardware encryption, (2) operating system encryption (such as Windows and Apple OS X), and (3) encryption software.

All hard drive manufacturers now offer drives with hardware full disk encryption, called Self-Encrypting Drives (SED). There are encrypted options available for both traditional hard drives and newer solid state drives. The major laptop manufacturers all offer models with hardware encryption. Hardware encryption generally is easier to use and administer than encryption software. Some examples of drives with hardware encryption are Seagate Secure and Momentus (*http://www.seagate.com*), Hitachi Self-Encrypting Drives (*http://www.hgst.com*), Western Digital (*http://www.wdc.com*), and SanDisk (solid state)(*http://www.sandisk.com*). Secure use simply requires enabling encryption and setting a strong password or passphrase. The contents of the drive automatically are decrypted when an authorized user logs in. It is automatically encrypted when the user logs off or the laptop is turned off.

Some IT professionals have recommended avoiding SED encryption because of concerns that data may be more difficult or impossible to recover in the event of a drive failure. They recommend encryption using one of the other options. With SEDs, backup of the data is particularly important.

Dell and Hewlett-Packard (HP) offer security suites that provide encryption, strong authentication, and additional security features. Dell's security package is called Dell Data Protection. It includes a number of separate options, ranging from strong authentication and encryption for a single desktop or laptop, to enterprise and cloud management tools. HP's suite is called ProtectTools. It also offers a number of options, from protection of an individual desktop or laptop, to central enterprise management.

Windows

Windows 7 Enterprise and Ultimate, Windows 8 and 8.1 Professional and Enterprise, and Windows 10 Professional and Enterprise include an encryption feature called BitLocker. BitLocker works below the Windows operating system and encrypts an entire volume on the hard drive. This means that when the drive is encrypted, the encryption protects the operating system, as well as all software and data on the drive. For versions of Windows that do not support BitLocker, software encryption, discussed subsequently, can be used.

On versions before Windows 8.1, BitLocker required either a computer that is equipped with a Trusted Platform Module (TPM) chip or use of an external USB drive to hold the decryption key. A TPM module is a security chip on the computer's motherboard that supports encryption. If a user plans to use BitLocker on a computer, it is important to select one that has a TPM chip that meets the current specification. Check the hardware requirements for the version of Windows that you are using and compare it with the specifications for the desktop or laptop. Or ask someone for advice—the major PC manufacturers have chat features on their Web sites to answer questions about their products. Use of a key on a USB drive is less secure because encryption can be defeated if an intruder gains access to the USB key. With Windows 8.1 and Windows 10, there's another alternative for BitLocker with computers that don't have a TPM chip. It can be set up directly on the computer, but it requires a pre-boot passphrase that accesses the decryption key. This means that a user has to enter a pre-boot passphrase, then log into Windows. A user can set up the same passphrase for both, but it has to be entered twice, once for pre-boot and once for logging in.

The business versions of Windows also include an encryption function called Encrypting File System (EFS). It allows encryption of files and folders. An authorized user who is logged in has access to decrypted data. It is encrypted and unreadable to anyone else (unless they can defeat the login process). EFS is considered a fairly weak encryption method that is easily cracked using forensic tools. You are better off using BitLocker or one of the other third-party encryption products discussed subsequently.

Setup of BitLocker is fairly technical. For many attorneys, it will be necessary to obtain technical assistance to implement it. There are instructions on Microsoft's Web site. During setup, there is a set of dialog boxes that take a user through the process. The instructions for different versions of Windows are available at:

- **Windows 10:**
  https://windows10-update.blogspot.com/2014/11/how-to-turn-on-bitlocker-in-windows-10.html
- **Windows 8.1:**
  https://technet.microsoft.com/en-us/windows/jj737997.aspx
- **Windows 7:**
  https://technet.microsoft.com/en-us/library/dd835565(v=ws.10).aspx

The BitLocker setup instructions include the following warning:

> Warning: When you turn on BitLocker for the first time, make sure you create a recovery key. Otherwise, you could permanently lose access to your files.

A Bitlocker recovery key is a line or set of data that can be backed up to a Microsoft account, a law firm network, or another computer. It also can be printed on paper. Make sure that the backup location is secure or the recovery key could be used to compromise the encryption. A BitLocker recovery key looks like this: 609430-136796-639472-379917-216106-640223-465533-702097

When backing up the recovery key, the drive identifier will be saved in the text file along with the actual BitLocker recovery key. If you have multiple partitions on the hard disk or multiple drives, you need to back up the key for each partition and drive. When utilizing the recovery key, you will need to match the appropriate identifier code to the correct drive. Windows 8.1 and 10 have an additional encryption option called Device Encryption. It's included in all versions of Windows 8.1 and 10, not just the business ones. It has very specific hardware requirements that most current PCs do not meet. It also requires InstantGo, a feature that allows a PC to instantly wake up. For information about these requirements and whether a PC meets them, compare the requirements on Microsoft's Web site with the manufacturer's specifications for the PC or ask someone for help.

Device Encryption is automatically enabled when a user with an administrator account logs on to a Microsoft account. The recovery key automatically is backed up to the Microsoft account. Although this option provides strong security for a PC, there is a risk that an unauthorized person can defeat it by getting access to a user's Microsoft account and the recovery key.

Device Encryption also can be turned on manually and the recovery key backed up to a network with Active Directory (a special purpose database for Windows networks used for authentication and authorization). There does not currently appear to be an option for enabling

Device Encryption without a Microsoft account or network with Active Directory.

Apple OS X

Older versions of Apple OS X have built-in file encryption in FileVault. Newer versions, starting with Lion, have full disk encryption available in FileVault 2. Follow Apple's instructions for turning it on. After a password is set, it just requires turning on the FileVault button in System Preferences. Instructions are available at *https://support.apple.com/en-us/HT204837*. FileVault 2 also generates a recovery key that it prompts the user to store. It provides an option for storing it with Apple.

Recent advances have attacked Apple's encryption scheme, and the Passware software suite claims to be able to defeat FileVault 2 in less than an hour. However, in order to use this tool, you must have a physical memory image file (acquired while the encrypted volume was mounted). Unless you're a forensic technologist, you won't even know how to create the physical memory image file, which is a forensic image of the memory contents of a running computer. Even with the availability of forensic tools, a laptop encrypted with FileVault is still far more secure than one without encryption.

Encryption Software

The third option for disk encryption (in addition to self-encrypting drives and operating system encryption) is encryption software. Some commonly used third-party encryption software products for hard drives include those offered by Symantec (PGP and Endpoint; *http://www.symantec.com*), McAfee (Endpoint Encryption; *http://www.mcafee.com*), Check Point (ZoneAlarm DataLock; *http://www.zonealarm.com*), WinMagic (SecureDoc; *http://www.winmagic.com*), and Sophos (SafeGuard; *http://www.sophos.com*). These vendors all have options available for Macs.

Most encryption solutions have single sign on options, where entry of the logon credentials automatically enters them for Windows or OS X. An open-source encryption program that was formerly widely used is TrueCrypt (*http://www.truecrypt.org*). However, it has been discontinued and should no longer be relied on. Its developers have posted the following on the TrueCrypt Web site:"WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues."

Group Policy

Many of the security measures discussed previously can be forced on users of your network. Why leave security in the hand of your users when you can require it? It's much easier to configure your requirements and push those settings out to the computers of your domain. To do this, you can use Group Policy Objects (GPO).

The obvious first question is: What is a GPO? Basically, a GPO is a policy to define user and computer configurations in a Windows environment. You can configure a GPO at the site level, domain level, or organizational unit (OU) level. They work by forcibly setting user and computer registry values. Because almost all of a Windows computer system is controlled through the registry, you have a lot of options when setting these policies. We'll attempt to give you some examples of common usages for GPOs and even some standard controls that should be implemented in every law firm.

If reading the previous paragraph already has caused your eyes to glaze over, be forewarned that this is not a sexy topic—which is one reason why you don't see too many articles about GPOs. But they are doggone useful, so get yourself a double shot of espresso and read slowly to get information you really can use in your law practice.

Can you control and restrict a Mac computer with a GPO or is this only for Windows systems? The simple answer is that it is much more difficult and complicated to achieve the same types of control and configuration for a Mac than it is with the embedded capabilities of a Windows computer. One solution is to integrate Open Directory with Active Directory. This requires a Mac OS X Server, which a lot of firms don't have. To make matters worse, Apple has announced that it is discontinuing its Xserve product line and may stop producing other server products. Another option is to purchase a third-party product such as Mac Management from Centrify.

We'll talk about using GPOs in a domain environment, which means you are running a Windows server on your network. Many of the things we'll mention also are available for stand-alone computers running Windows 7, 8, or 10. Obviously, if you have a server-based environment, the preference is to centrally manage users, computers, and applications. It is much more time and cost-effective to centrally manage Group Policies through Active Directory than it would be to run around to every computer and set the local policy. These Active Directory based GPOs also are known as nonlocal GPOs. They are created in Active Directory and stored on a Domain controller, such as a Windows 2012 or 2016 server.

Tools

How do you create and manage a GPO? The process varies depending on the server Operating System, but typically you would use the Group Policy Object Editor from Active Directory.

Generally, you will then need to edit the Default Domain policy. Windows 2008 domains also have a Default Domain Controllers Policy. The Default Domain Policy already has a lot of built-in objects that can be edited very easily.

Group policies can become very complicated, especially in larger environments. You will want to be familiar with the Group Policy Results (GPResult.exe) command line tool to troubleshoot Group Policies implementations. You start by opening a command window. This is done by clicking Start, Run and enter cmd to open a command window. Typing gpresult in the command window will show you all of the optional parameters that are available. A very common entry would be gpresult/r to generate a report to the command window. The report will show such things as the operating system that is running and any policies that are in effect.

Policy Inheritance

A large number of problems with GPO implementations arise from a lack of understanding about inheritance. You do have the option of blocking inheritance, but we think that makes the situation even worse. If you leave the default inheritance enabled, then you can just follow the flow through the Active Directory "tree" to see where the problem may lie. GPOs inherited from the Active Directory are always applied over the local policy. Even if a user has administrative rights to their computer, an administrator can overwrite anything they configure through the use of a domain policy. After that, the GPO that is closer to the object (*e.g.,* computer) is "stronger" and takes precedence.

Policy Updates

Group Polices from Active Directory are refreshed on the computers by several methods:

1. Logon to the computer (if the GPO settings are "user settings").

2. Restart of the computer (if the GPO settings are "computer settings").

3. Every 60 to 90 minutes when the computer queries the Domain Controller for updates.

4. Manually by using the gpupdate command.

Generally you will want to manually force the GPO updates while you are configuring and testing the policies. As an example, if you configured a GPO for a printer installation (yes, you can do that), you would want to see if you got it right. Configure the GPO, force the update, and then see if it actually works.

Types of Control

GPOs can do a lot to automate activity and control configurations of your computers. Some of the things that can be achieved are:

1. **Configure the user's desktop.** This could include all sorts of things such as device (*e.g.,* printer) installations, colors, etc.

2. **Configure local security on computers.** You can restrict access to specific folders on the machine or whether the last logon name appears.

3. **Install applications.** This is a great activity, especially for deploying new applications to a bunch of computers or sending out updates. Besides installations, you also can remove the icons and ability to run certain programs such as the built-in games that come with Windows.

4. **Run startup/shutdown or logon/logoff scripts.** You can have certain activities occur when the machine is started or shut down. As an example, all temporary files can be cleared when a user logs off the computer.

5. **Configure Microsoft Edge settings.** You can set a default home page for the user's browser.

6. **Redirect special folders.** You can assign drive letters to specific folders.

Common GPOs

Now we'll get to the more interesting items that you've been waiting for. We implement GPOs for the majority of our clients and even do some special activities as they request. Several of the GPOs we implement are for security and confidentiality reasons. The rest of them tend to be for application management or standardization within the firm.

Last Logon ID

One of the GPOs we highly recommend is removing the display of the last user ID that logged onto the computer. Typically, you will logon to a computer using a user name and a password. By default, Windows will leave the user name populated with the last ID that was used to logon to the computer. This means that only one more piece of information (the password) is needed to gain access to the computer and therefore data on the

network. By removing the display of the last logged on user, two pieces of information (user ID and password) are needed. This makes it harder for someone to compromise your systems because they'll need both items for a successful logon.

Password Length

Another object we define is password length. At the present time, 14-characters is the recommended password length.

Password Expiration

Passwords should expire after a period of time, thereby requiring that they be reset.You're familiar with this concept if you do any online banking. Periodic password changes help maintain security of the system, but it looks like NIST will be changing that recommendation.We currently set the password expiration at 30–45 days.

Password History

This value defines how much time must pass before you can reuse a password.This is to prevent a user from changing the password (because it expired) and then changing it back to the old value. That would defeat the purpose of the expiration period. We set this value at 24 months, which means we will never see the same password being used for at least two years. Some users will object to this policy and complain that they can't remember their passwords. Resist the temptation to soften this policy. Perhaps changing the expiration period to a longer time would be a good compromise, or better yet, use a password manager.

Account Lockout

There are several GPOs that can be set for this.The Account Lockout Threshold is the number of times an incorrect user ID/password can be typed in before the account is locked out. A number between three and five should be sufficient to account for honest mistakes and typographical errors. The Account Lockout Threshold is important to stop attempts by a computer program or person trying to gain access to your computer systems.

The Lockout Duration is the period of time that the account remains locked following the number of invalid logon attempts as set by the Threshold value. If you use a value of zero, the account will remain locked until it is manually unlocked by the administrator. A Lockout Duration of 30–60 minutes is an acceptable period. This will be sufficient to stop hackers or botnet computers from guessing user ID and password combinations.

Folder Redirection

This is the GPO where the system folder contents for the user are redirected to a central storage area on the server.This allows the user to use any computer and have their information stay consistent. Examples of the types of folder redirection contain the following:

- **Application Data.** This folder contains the user configuration files, the user-specific data that is utilized by applications and PKI files. By redirecting this folder, the user does not need to be configured again when they change systems. Their applications will work in exactly the same way no matter which computer they use.
- **Desktop.** This folder contains the files and shortcuts that appear on the user's desktop.
- **My Documents.** This folder contains the files and pictures for the user.This means the user can access any of these files from any computer.
- **Start Menu.** This folder contains the shortcuts and files that appear on the Start menu.

Temporary Files

Several of our clients want to clear the temporary Internet files for each user. We configure a GPO to clear the temporary Internet files when each user logs off.

Application Deployment

A very valuable feature of GPOs is the deployment of applications.We've used this ability to roll out new versions of Office to every computer, distribute the antivirus software, and quickly distribute any software or patches within the firm. It takes a little work to configure and test a GPO, so there should be several computers that need distribution before expending the effort. As an example, it's probably not worth implementing a GPO to distribute QuickBooks to one computer. However, pushing out an update for Tabs3 to hundreds of computers is worth it.

Smartphones

Lawyers, for the first time in memory, are at the technology forefront, with more than 92 percent of them owning smartphones. Smartphones are extremely powerful devices, capable of storing contacts, calendar entries, email communications, electronic files, voice messages, and a host of additional confidential client information. As an attorney, you have an ethical obligation to protect the client data that is stored on your

smartphone. Here are some security tips for protecting the data and some easy measures designed to avoid having the device and data compromised.

Smartphones are extremely powerful devices, capable of storing contacts, calendar entries, email communications, electronic files, voice messages, and a host of additional confidential client information. As an attorney, you have an ethical obligation to protect the client data that is stored on your smartphone.

Encryption

Such a simple word, but most attorneys are petrified at the thought of having to encrypt anything and avoid it like the plague. Encryption is simple and very easy to accomplish on a lot of smartphones. Just setting a PIN on an iPhone enables encryption and many Android devices have encryption capabilities as part of the operating system installation, with the latest versions working just like the iPhone by encrypting when a PIN is configured. Bottom line: Enable encryption and you'll go a long way toward protecting the data on the phone.

Encrypt Expansion Memory

Besides the main memory, be sure to encrypt any memory expansion cards that may be used. iPhone users don't have to worry about this because you can't expand an iPhone, but others need to protect any data that may be saved to the card.

Lock Code

Be sure to set a lock code for your smartphone.This will help prevent unauthorized access to the information. Set a code that is longer than the typical four or six-digit PIN to make it more difficult to crack the number. For iPhone users, turn off "Simple Passcode" in order to enter more than four or six digits. Better yet, use a password instead of just numbers.

Inactivity Timer

Set a fairly short inactivity timer for your smartphone.This automatically will lock the phone if it hasn't been used for a period of time. Don't be tempted to set your timer at five or more minutes.You should configure the value to be no more than two minutes. Many attorneys complain that the phone will lock too quickly with such a short value, but larger numbers leave you exposed should you leave your phone in the cab (one of the authors has done that).

Location Services

Turn on the location services of your smartphone to facilitate finding the phone if it is ever lost. iPhone users would enable the "Find My iPhone" feature through iCloud. The ability to locate your smartphone must be turned on before you lose your phone, something many lawyers seem unaware of. Location services are included in the latest versions of the Android OS, so no add-on product is required as with older outdated versions. Even if location services are not enabled, you can still send a message to the device or have the smartphone play an alert sound, even if the sound is turned off or the phone is in vibrate mode.

Remote Wipe

Make sure you have the ability to remotely wipe the phone should you lose it. This is different from being able to locate the phone. Remote wipe means you can remotely send a command to wipe the information from the phone. Remote wipe is part of the "Find My iPhone" feature for iPhones and included in the more recent versions of the Android OS.

Security Software

Security software for mobile devices is no longer an option. Malware writers are now targeting smartphones in a major way. All of the major security software vendors have products for the popular manufactures and models of smartphones, and you may be able to purchase an add-on license for your firm's current security suite.

If you're looking at standalone solutions, Lookout is a great free security application for Android devices. We also recommend a security product called Sophos Mobile Security for Android (*https://www.sophos.com/en-us/products/free-tools/sophos-mobile-security-free-edition.aspx*). Specifically designed for Android, Sophos Mobile Security identifies malicious or potentially unwanted applications that could result in data theft, data loss, and excessive network usage costs. If your device is lost or stolen, a remote lock or wipe will shield your personal information from prying eyes.

iPhone users pretty much have to trust Apple because they don't allow any third-party access to the core of the operating system with iOS 9 and earlier devices. iOS 10 now allows some access to the operating system kernel, but security vendors are just beginning to take advantage of the change.There are security products for the iPhone, but they are not real-time scanners such as those available for the other smartphone operating systems.

URLs and QR Codes

This security tip doesn't require any specialized software or hardware device. Our advice here is not to click on any URL that you receive in a message (email or text) that you are not familiar with. Also, we're not big fans of any shortened URL (*e.g.*, tiny URL or bitly) because you really don't know where it will take you. The same goes for QR codes. The QR code is a picture-type barcode and you really don't have any clue where the code will take you.Think of it as the "Wild, Wild West" of the Internet. On the plus side, the previously mentioned Sophos mobile device security software checks to see if the QR code is safe.

Wireless Networks

Many smartphone users will connect to wireless networks in order to avoid the data charges associated with accessing the 3G/4G data network of the cellular provider. Using wireless networks is not a problem, but make sure you are connecting to a secure wireless network. Many of the free wireless networks available at businesses (McDonald's, Starbucks, etc.) are open networks with no encryption. This means that someone else could be monitoring the network traffic and capturing your data transmissions. This means you should only use secured wireless networks. WPA2 encrypted wireless networks are the only recommended connections.WPA encryption was cracked long ago and WEP encryption can be broken in a matter of minutes.

Update Your Device

Always run the latest version of the operating system for your smartphone. Just like your computer, vendors provide updates for the operating system to patch security vulnerabilities and add additional features. iPhone users can get the latest updates through iTunes or through over-the-air (OTA) updates. Other users typically get the updates directly from the cellular provider. You may not have a choice when it comes to updates as the carrier may force it to your phone.There doesn't seem to be any consistency with the operating system updates.We've had Windows Mobile phones for which we had to manually download updates from the carrier's Web site. Our BlackBerry smartphone was updated by checking for updates from the phone, which would download them directly from BlackBerry. Finally, our current Android phone has updates pushed to it automatically from our cellular provider or you can manually check for updates from the phone.

Don't Jailbreak or Root

Do not attempt to bypass the security or normal operation of the smartphone by jailbreaking or rooting the phone. Bypassing the security certainly makes you vulnerable to potential compromise.

Application Installations

Be wary of any applications from unknown sources. The applications available through iTunes are pretty safe, but there have been several instances when malware has slipped past Apple's review process. Google has been criticized for letting malware-laden applications "camp out" in their store, but it has improved policing application safety through Bouncer. Bouncer still isn't bulletproof and some malware is still slipping into Google Play. Just make sure you review what others say about an application before you load it, which should help you stay out of trouble.

The application may want to record your phone number and location. It may have the ability to actually make a phone call without your involvement. Some apps even say they will access your contacts.

Terms of Service

It still amazes us that lawyers tend not to read the terms of service. They will read contracts for their clients, but not for their own use. The Terms of Service will tell you what you are agreeing to, which in turn tells you what the application wants to do.The application may want to record your phone number and location. It may have the ability to actually make a phone call without your involvement. Some apps even say they will access your contacts. Reading the Terms of Service could keep you out of trouble by protecting access to your data when you realize all the information that the developer wants to access. On a regular basis, we are mystified by some of the functions that apps demand.

Turn Off Unneeded Interfaces

This helps conserve battery life. Turn off anything you don't need or use at the moment. As an example, shut off the Bluetooth if you are not using it.You also should shut off the Wi-Fi radio if you are not connected to a wireless network.

Mobile Device Manager

You may need a Mobile Device Manager (MDM) to enforce policies on the smartphone.Whether you purchase a MDM or not, something should be in place to enforce and control certain aspects of the smartphone. Items such as enforcement of a password, password

complexity and length, encryption, inactivity timeout, etc. should all be required items and the user should have no option to bypass them.The ActiveSync policies available with a Microsoft Exchange server should be sufficient for most small firms. If your firm subscribes to Microsoft Office 365, an MDM also is included to manage the security of your firm's smartphones.

Backup

Backup your data and applications. iTunes (not iCloud) should be used for the backup of iPhones. This is because iTunes provides a local backup (which can be encrypted) and because the iCloud's Terms of Service are not security-friendly, along with the insecurity and inherent dangers of the iCloud (remember "Celebgate?"). If given the option, you always should encrypt the backup. There also are third-party applications that can be used for backup.Why backup? Because this is another layer of protection should you misplace your smartphone and have to remotely wipe it.

Conclusion

Managing technology and cybersecurity is never-ending.You cannot "set it and forget it."At least annually, you need to review your technology (what needs upgrading? Is anything out of support and not receiving security patches?, etc.). Keep reading legal tech resources. Attend CLEs to stay current.Talk to your colleagues about what they are using to enhance their practice of law and to keep their data secure. In the end, be prepared to recover from calamity.As many law firms have discovered to their chagrin, calamity can be just around the corner.