CYBERSECURITY:

How to Keep the Hackers at Bay

(800) 367-2577
www.alpsnet.com

ALPS

Written and Presented By:

Mark Bassingthwaighte, Esq.
Risk Manager, ALPS

Presenter Biography

Kurt Whitmire, Business Development

Coming to ALPS with an extensive business background, Kurt brings a unique perspective on liability insurance to his role in business development. Having owned his own business Kurt understands what decision makers value. While liability insurance isn't top of mind for every law firm on a daily basis, choosing the right carrier is certainly an important decision to make when the time is right. As a business owner, Kurt was working with partners that he knew would take care of his business when he needed them most. He understands that the firms he works with want the best value for their hard earned dollar and the peace of mind knowing that the firm can always rely on their partners. This relationship is often sold to firms but it is not always delivered. Kurt's role at ALPS is to be a conduit between law firms and ALPS' staff of underwriters, claims attorneys and others to deliver on ALPS unique and time-tested value proposition.

Contact Kurt at (800) 367-2577 or kwhitmire@alpsnet.com.

Table of Contents

Resources

Just Because You Can Do Something Doesn't Mean It's a Good Idea.

An attorney's decision to use an iPad, a cloud based service such as Dropbox, a smart phone, a Wi-Fi network, or even basic email in the furtherance of delivering legal services is not in and of itself unethical nor a poor business decision. The real problem is with what those who use such tools do or don't do with them. Portable devices, to include backup drives, are sometimes lost or stolen; rogue programs that capture banking passwords, encrypt your data, or steal your data can be unintentionally downloaded; your network resources can be used in a hacking attack; and this list could go on and on. Much of the risk comes from missteps such as lax security procedures, falling victim to a social engineering attack, and even simple ignorance about how a given device works or what the application really does.

Now we've all seen the headlines. Who hasn't heard about the Google docs phishing scam, the CIA WikiLeaks dump, the Netflix breach, and Putin's attempt to influence elections around the world just for starters? Yet it's what isn't making the headlines that should have our attention. A recent survey of 300 IT professionals in the U.S. and U.K, done by Vanson Bourne, found that 84% of respondents were victims of a spear phishing attack with the average cost of the attack coming in at $1.8 million. Security company G Data has recently reported that 8,400 new Android malware samples are discovered every day. In short, a new instance of Android malware pops up nearly every 10 seconds! Taken together, one can surmise that cybercrime is going to continue to be a serious concern for the foreseeable future. Not be pessimistic, but my personal perspective on the odds of a law firm having to deal with the fallout of a security breach is this. It's not if it will happen, it's solely a matter of when; and if your response happens to be "we're too small to be on anyone's radar," please understand that a significant percentage of cybercrime attack vectors are automated. The size of the target isn't part of the equation. It's simply about taking as much data or money that the hacker can.

The real issue that must be addressed given that these kinds of breaches are occurring is this. What might the fallout be for any attorney or firm whose system is involved in a data breach event? After all, if client confidences or funds are lost while in possession of an attorney, would not liability for any resulting harm to the client fall on the attorney? Of course, it would.

Cyber Crime; Your Ignorance is Their Power

Before we move to a more thorough discussion of liability for a data breach, one must first understand that the goal is to avoid having to deal with the problem in the first place. Unfortunately for most attorneys it is their ignorance, as well as that of everyone

else in their office, that's the real problem. Regardless of all the precautions implemented, from taking steps like securing all digital assets with the latest and greatest in firewalls and antivirus software to upgrading to the latest in browser software or operating system, those efforts still aren't going to be good enough. There is a weak spot that IT support can't easily address and can't be fixed by throwing a little more money at it. The true vulnerability comes from the folks who use the tech. I'm talking about you, your paralegal, your receptionist, and anyone else who has access to or uses a firm computer, tablet, smartphone, and the like. How do you think the Yahoo breach, the DNC email scandal, and many of the other ones we hear about with ever more frequency, happen? In short, someone does something stupid like open an email, click on a link, or verify a password because he or she doesn't know any better or they get caught off guard.

To help bring the point home, ask yourself these few questions and focus not only on how well you can answer them but also think about how everyone else in the office might do. Do you know what Cerber and Dridex are? (Cerber is ransomware that encrypts files on every drive it has access to and Dridex is a banking trojan that seeks to steal your online banking credentials.) If you did know what these two examples of computer malware were, do you know if you can still be infected by either if you have an Internet security software suite running? (Yes, until a patch is released for each new variant that is discovered in the wild; but be aware that malware is rapidly moving into the mobile space where many are woefully unsecure.) Can a computer attack start with a simple phone call? (Yes, it's called a phishing phone call.) What is spear phishing? (Targeted attacks that appear to come from a trusted source.) Can identity theft occur via a text message? (You bet.)

Hopefully you start to see the point. As users, our actions can unintentionally circumvent the security tools that have been deployed and often it happens out of sheer naivety. Someone is uninformed and a cybercrime can occur as a result. What any of us do on the Internet and even how and where we do it actually does matter. For example, unsecured Wi-Fi is exactly that, unsecured. Just because a signal is available doesn't mean using it is a good idea. Cybercriminals have the same ability to access that signal as you do and how would you know they're there waiting for you? Again, perhaps you are smart enough to avoid most attacks but how about everyone else in your office? Do you know what they are doing online or with their mobile devices?

What's the solution? How does one address the very real threat that comes from each and every user? I wish it were easy. Unfortunately, it isn't; but it is manageable. This is one of those situations where IT and firm attorneys need to work together. Part of the solution will lie in periodic training in safe practices to include how to identify threats. This needs to be ongoing because the attack vectors will continue to evolve and change. Topics

such as what do the latest social engineering attacks look like and how can they be avoided, why peer-to-peer file sharing networks like the ones that use a BitTorrent protocol can be dangerous, and how to securely login into the network from a remote location would all be worth discussing. Personally, I would start with a short session that teaches everyone how the particular security program you run on your network would respond should an actual threat be detected. What will that look like to the user and what should they do if it happens? Why do this? How many of your users know that if and when a pop-up box suddenly appears informing them that their computer is infected and telling them to click "yes" in order to start a scan is not, in fact, your security software doing its job? Instead, this can be an actual ransomware attack. If the user actually clicks on "yes," truly believing that this is the right thing to do in order to protect the system, that act will initiate the malicious program. Trust me, that's not what you want to have happen.

Another part of the solution will be in establishing and enforcing a firm wide Internet use policy that spells out the dos and don'ts. Define what might be acceptable to download and what wouldn't. Allowing someone to download an eBook off Amazon might be ok if they were to do it over the noon hour, but downloading free stuff along the lines of screen savers, emoticon programs, desktop wallpaper, and even music may not be the best idea. What about accessing Facebook, LinkedIn, Snapchat or Pinterest from an office device? There are security concerns that come with participation in social media. Do you want to allow access to things like Skype, YouTube, or even personal email accounts? In the absence of defined rules, there will be some who will expose the network if for no other reason than through naivety. Also, don't focus just on the Internet spaces listed here. They are simply examples. All can bring value but all also bring a certain amount of risk.

Again, there is no easy solution, and unfortunately there is a catch 22 for many attorneys. For example, there is often a temptation to simply block access to something like Facebook; but this may be a bad idea because there will be times when visiting Facebook will be absolutely called for as part of handling a client's matter. The good news is that a great resource is available online to assist in the identification of the issues as well as in the development of a firm policy or policies. For additional information see www.sans.org/security-resources/policies/.

The final piece will be in committing to seeing that systems and software remain as current as economically feasible. Why? If you have an older version of a program still in use at your office do you know if it is still being supported? As newer and more secure versions of software come to market, software companies eventually stop supporting the older versions. Now this doesn't mean the program stops working; but it does mean the security updates stop coming. Continuing to rely on older software in order to save a little money is a serious misstep because many malicious programs specifically target older software.

Cybercriminals know that the vulnerabilities in these older programs will never be addressed and that works to their advantage. Don't make it easy for them. Understand that when it comes to computer security, newer and better solutions for hardware and software will continue to enter the marketplace. When you think about what is at stake, isn't the investment cost of updating to the most current version of a software program available well worth it?

The Goal is to Avoid the Breach

Clearly computer security cannot be an afterthought and, as has been discussed, there is no one-step solution that will adequately address the problem. Maintaining data security is going to be a never-ending effort that will involve everyone in the firm from the part-time receptionist to the most senior partner.

Beyond the obvious business reasons that one should address cyber security, understand that as attorneys we also have new ethical duties that have come into play. Under CO RPC 1.1 Competence, a lawyer's efforts to provide competent representation now includes an obligation to keep up with changes in relevant technology. (See comment [8] to Rule 1.1 which states "*To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, and changes in communications and other relevant technologies...*") We must also preserve and maintain client confidences under CO RPC 1.6 Confidentiality of Information which now states in section (c) that "*A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client*" and Comment [18] under Rule 1.6 now states the following. *"Paragraph(c) requires a lawyer to make reasonable efforts to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision.*"

How far must a lawyer go when it comes to complying with these rule changes? Fortunately Comment [18] of CO RPC 1.6 provides something of a safe harbor: "*The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult*

to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule."

With all this in mind, it would seem that attorneys do have an ethical obligation to take at least basic steps to become cyber secure, which means taking steps to protect data, particularly critical or sensitive data. The data of most concern would include personally identifiable information to include social security numbers, names, birth dates and the like; financial information which might include account passwords, credit card information, personal health or medical information not only of clients but of staff and attorneys as well; and of course, client confidences. The challenge here is in understanding that the obligation to protect data means that steps must be taken to protect your systems from data corruption, unauthorized access, and unauthorized use; and you must address these issues as it relates to email, cloud storage, document collaboration in the cloud, the use of Wi-Fi, the use of personal devices (smart phones, tablets, home computers, laptops, jump drives, etc.) and the list goes on.

Data Security – It Starts Here So Stop Making Excuses

The days when a lawyer could send an unencrypted email without worry, remain blissfully ignorant about encrypting a laptop, or use the same easily remembered password for all accounts and devices are over. I believe most lawyers know this, at least at a gut level; but far too many still seem to be confused about what steps they should be taking. If you see yourself as a card-carrying member of the "what the heck am I supposed to do" group, perhaps I can help.

Let's start with email. It isn't secure. The best description I've ever heard about how anyone should view email was this. Email is like sending a postcard written in pencil. Slap a little postage on it, drop it in the mailbox and it's good to go. Think about that and then think about your ethical obligation to preserve and maintain client confidences. Still want to email a client confidential information using a free Gmail account? Hopefully not!

Encrypted email is on the horizon for all of us and a day-to-day reality already for some. Certain clients (the financial and healthcare sector for starters) are beginning to demand the use of encrypted email. Say no and lose a client. Is the use of encrypted email ethically mandated at this point? No, but I personally believe that's coming, if for no other reason than the market will demand it. Until that time, however, here's an easier solution.

When using email to send confidential information, place the confidence in a Word document or PDF file, password protect that document and attach it to the email. Now the

attachment is encrypted even though the email itself is not. There are various other security settings that can be selected as part of this process and those vary depending upon the application in use. Learn what they do and how to use them. Now, one side note. Never put the password to the attachment in the text of the email itself. You'll need to find another avenue to pass that information along and that's just the way it is. Provide the password that will be used during the course of representation during intake or perhaps a text message or quick call will take care of it. Also understand that if the password is ever lost or forgotten, you won't be able to recover the contents of the document so don't get casual with this.

You also need to address the issue as it relates to mobile devices, backup storage media, and placing documents in the cloud. I'm going to skip all the "put the fear of God in you" stories and ask in return that you put aside all the excuses. I believe you know what you should be doing. It's just a matter of making the decision to actually do it.

Smartphone encryption is pretty easy. On newer smartphones, encryption is often a matter of changing one setting. On the iPhone, enable the complex password setting, and for Android phones, enable encryption in settings. This basic step doesn't necessarily encrypt everything on your phone so I would strongly suggest you review the security instructions of the device manufacturer and carrier, which means you need to go further than reviewing the quick start guide. The information you need to know is not there. And yes, I do understand this means you have another password to remember; but if your phone is lost or stolen and a client is harmed in some way as a result, they are not going to be sympathetic once they learn the phone wasn't encrypted because you didn't want to have to remember a password. After all, would you if you were in their shoes? I doubt it.

Tablets and laptops can be a bit more difficult to set up but most of these computers have full disk encryption functionality built-in. It's just a matter of turning it on. If you don't consider yourself tech savvy, however, this is the one time I would advise you to get a little help from your IT support so that it's done correctly. Once setup, it's easy as long as you never forget the password. Even better, these built-in encryption programs can often be used to encrypt backup drives. This is what I do for my personal back-ups. Takes me all of 5 seconds to decrypt a drive and run the next backup. There are also a number of third-party products (e.g. Backup Exec or BounceBack Ultimate) and cloud based solutions (e.g. Mozy or Carbonite) that are just as effective. If you do decide to go with a cloud-based vendor, make certain that you select the password because you don't want the vendor to have the ability to decrypt your data.

While placing documents in the cloud is convenient, it also brings about privacy and security concerns which, again, can be easily addressed through encryption. The condition,

however, is you must be in control of the decryption key, not the cloud service provider. If you don't control the decryption key, you don't control your data. It's as simple as that. Some cloud service providers, for example Box, provide for end user controlled encryption. If your cloud service provider does not, you must take the time to encrypt your documents before placing them in the cloud. Products such as BoxCrypter, Sookasa, and Viivo can get you there.

I'm well aware that I'm only focusing on encryption and acknowledge that there are all kinds of other steps one can and should be taking to protect your data. I elected not to share all the other tips here because encryption is the ultimate level of protection should something bad happen. Systems and devices can be lost or stolen, and worse yet, hacked in all kinds of ways. Encryption is your failsafe should something bad ever happen. Think about it this way. Your clients expect that you will protect data about them just like you expect your credit card carrier, your medical provider, your bank, or your insurance company to protect information they have about you. You read the headlines, learn from the missteps of others. Stop with the excuses and just do it.

Obviously, the challenge with all the above and, truth be told, the success of the effort relies upon the use of complex passwords that are never used twice and there's a relatively easy solution to this problem as well; but first a story.

When Passwords Fail – A Personal Story

Sometimes married couples see things differently and the only way to resolve the tension is by finally deciding to agree to disagree. That's how things played out in our home for a number of years on the issue of passwords. My wife seemed to view my focus on computer security and passwords as something approaching mild paranoia. I, on the other hand, viewed her insistence that the use of one easily remembered password for everything in her life was like tattooing the words "victim here" on her forehead. The only way for us to move forward on this issue was to agree to disagree and that's just what we did.

This state of marital bliss started to crake a few years later after I received an email from one of our sons letting me know my wife's email account had been hacked and a bunch of spam was being sent out using her email address. I did what one normally does to remedy that situation and hoped all would be good. Sadly, it wasn't to be. Our marital bliss abruptly ended a few months later after we received written notice from a credit union on the opposite side of the country telling us that they were most displeased with my wife. Apparently credit unions don't like it when someone gets a new credit card, immediately

maxes it out, and then fails to make any payments. Makes sense to me. Problem was she wasn't the one who walked into that credit union and applied for a card in her name.

While this tale has many more interesting twists and turns, in the interest of time I will simply share that as a result of this identity theft a federal and an out-of-state tax return were also fraudulently filed in her name. I spent over three years working to get everything cleaned up; but the one thing I can't do, and honestly no one can, is ever get her identity back. That's been taken and we'll have to deal with the ramifications of that for the rest of our lives. Hopefully, it's over; but only time will tell.

Today things are different around here. My focus on computer security is viewed in a much different light and my wife needn't worry about any unsightly tattoos on her forehead. While we've returned to a state of marital bliss, this time around we're both on the same page.

Now understand that this entire saga started with someone managing to figure out a password and that password opened all kinds of doors that were supposed to be locked. I chose to share this story because I wanted to put a real-world spin on the problems that can arise when too little attention is given to the importance of passwords. I don't care if you are just a solo practitioner as opposed to the managing partner of a 50-attorney firm. Everyone needs a password policy, formal or informal, in order to try and avoid becoming yet another victim of identity theft, and heaven help you if the identity theft turned out to be the identity of one or more of your clients because someone got into your office network. So not good.

Let's start by talking about bad habits. Here are the kinds of things you should never do. Use the same password on multiple devices or applications. Write down the computer password on a sticky note and hide it in your laptop so no one can see it if it's closed. Believe that passwords like "qwerty", "password", "1234567", or "letmein" are clever and acceptable. They aren't.

The better approach is to develop a policy that everyone in your office, including you, will abide by. It should mandate the use of a strong password, which is currently defined as one that is a minimum of 14 characters long and includes numbers, special characters, and upper and lower case letters if the device or application you wish to secure with a password will accept it. In addition, every application and device in use should have its own unique password and, at least with mission critical devices and applications (e.g. banking login credentials), these passwords should be changed every 6 months. Never recycle old passwords and never share your user ids and passwords with anyone. Finally, always use two-factor authentication for any device or application that allows it.

Yes, keeping track of all these complex passwords can create its own problem. Fortunately, this problem can be easily managed with the help of a password manager such as RoboForm, LastPass, or Dashlane. Products like these can generate complex passwords and store them for you in an environment far more secure than a piece of paper hidden in your desk somewhere. In fact, my wife joined me in using password managers shortly after her kerfuffle with the credit union and it has made a world of difference. She still only needs to remember one password, albeit a strong one, to open the password manager and that's it. Compliance with our home password policy has never been easier for her, and speaking frankly, she fully agrees that compliance isn't optional. Trust me, she gets it now. The interesting question is, do you?

How to Not Become Yet Another Victim of Ransomware

Back in 2015, attorneys from two different firms spoke with me about being hit with a particularly nasty ransomware attack. In each case the firm's files were encrypted by CryptoLocker and thus unavailable. Both firms experienced about four days of down time, meaning they had no access to their computer network. Both have since recovered from the attack but this is where the similarities end. One firm ended up paying a ransom of $300 in bitcoin (a digital currency) in order to recover over 1 million encrypted files. The other firm elected to have their IT staff wipe their systems in order to rebuild from a clean backup that was about 30 days old. Yes, they lost 30 days' worth of work; but they did avoid having to pay the ransom. The firm was advised not to do so because there are no guarantees in paying the ransom and doing so can invite future attacks. I can assure you the involved attorneys slept little after the attack with a real worry that this, to use their term, "nightmare" wasn't going to end well.

If the above story made little to no sense to you, now's the time to become aware. Ransomware attacks are causing all kinds of problems for businesses of all shapes and sizes all over the world and law firms are not immune. That said, let's keep this simple because I'm not a computer security expert and if you're still reading this, the odds are neither are you. The bottom-line is this. You and all who work at your firm need to know a few things because your actions or inactions are often to blame for these kinds of attacks.

At its most basic level ransomware is a type of malware, think rogue software. These programs seek to prevent you from accessing your computer or your files until you do something, which is often pay a ransom. There are a number of different types of ransomware. Some encrypt files and others lock you out of your system. Anyone at your firm can allow an attack to initiate by naively clicking on an infected email attachment, innocently clicking on a fake security popup, visiting a hacked website, or clicking on a

malicious link on a social media site and it can happen in an instant. Unfortunately, no one may be the wiser for hours because encrypting all your files takes time. It's only after the encryption process has completed will you be made aware of the attack via a pop-up that demands the ransom payment. All I can say is these programs will continue to become more sophisticated and the ways attackers will try to trick the innocent into falling pray will continue to evolve so everyone at your firm must remain vigilant when it comes to doing their part to help protect your network.

There are a number of things you or your IT support can do to prevent these kinds of attacks. Keep your security software, internet browsers, and operating systems updated and make certain that all update settings are set to automatic on all PCs, laptops, tablets, and smartphones. Backup regularly and make sure that a current copy of the backup is not connected to the network because encrypting ransomware will look to encrypt all connected drives. If your backup happens to be an external drive that is always connected, it too will be encrypted. This is one of the reasons why rotating backup drives off site or backing up to the cloud is strongly recommended.

More importantly all network users, to include every attorney and staff member at the office, if they are not already aware, need to be trained on a few security best practices which will help keep your network safe, not only from ransomware, but from a wide variety of cyber-attacks. The following list would be a great place to start and understand that these rules apply not only to PCs, but to laptops, tablets, and smartphones as well.

Don't click on any links in emails or sent to you on social media sites. Criminals send links that appear to come from companies or persons you know and trust in order to try and trick you into clicking the link. Doing so can initiate a download of malware like CryptoLocker or take you to a fake website in order to attempt to steal your personal information. If you are uncertain as to the legitimacy of the email, try hovering your mouse over top of the URL in order to view the actual hyperlinked address. If the hyperlinked address is different than the address displayed in the message then the message is probably fraudulent or malicious. So, for example, if an email claims to be from FedEx but when you hover your mouse over the FedEx text the hyperlinked address that is displayed says something other than FedEx.com it isn't FedEx. Also, be aware that sometimes the domain name is altered. If placing the mouse over the FedEx text displays something like FedEx.com.malicousdomainname.com, this too isn't FedEx. If you still feel that you absolutely must see whatever the link is supposed to show you go to the site yourself. For example, type www.FedEx.com in your browser yourself or use a search engine to look up the correct URL of FedEx.

In a similar vein, don't open attachments unless you know and trust the sender and also know what the attachment is. Again, doing so can initiate the installation of rogue software on your system. If you're not sure about the authenticity of what has been sent to you might try the mouse hover approach detailed above. In the alternative, reach out directly to the sender and ask if they actually did send the email. If you are questioning why a lawyer whose name you recognize sent you some important document but you also don't have any recollection as to why it was sent, call the lawyer directly to ask about it and always lookup the number yourself. Why take the time to look up the number yourself? Think about it; if the email is a fake, the contact information provided in the email is fake as well. Don't be fooled! Other clues that a message is likely fraudulent or malicious include poor spelling and grammar, the message asks you to verify personal information, and or the message threatens you if you don't do something.

Only download and install software or apps from websites that you know and trust. Downloading free games, files off of file sharing sites, customized toolbars, and even things like free flashlight apps (which are often a particularly nasty snooping app that can only be removed by a factory reset of your phone) may seem like a great deal but they can bring real trouble with them.

Use a pop-up blocker and don't click on any links within unexpected pop-ups or buy software in response to an unexpected pop-up. Unexpected pop-ups are another way scammers try to trick people into downloading malware. On Windows systems, for example, simply close the pop-up from the task manager or click on the pop-up icon on the task bar and then click on close. As an aside, make certain that every person in the office knows that security programs do not need someone to click on "scan now" in a pop-up that states their system is infected. The security programs do that automatically. Really bad things can happen if they fall prey to this scam. In fact, this is how another of our insured firms got hit with CryptoLocker.

Have a policy that absolutely prohibits anyone from disabling their firewall or changing their browser security settings in order to allow a webpage to properly load. If a web page is not properly loading there is a valid reason. Disabling firewalls and changing security settings can allow a "drive-by" download, which is an automatic download of a malicious program that initiates as soon as someone visits a compromised Web page, to occur.

Finally, know the warning signs. If anyone's device slows down, crashes, displays repeated error messages; won't shut down or restart; will no longer update; starts showing a lot of pop-ups; displays web pages they didn't intend to visit; displays unexpected toolbars or shortcut icons on their desktop; if they experience a sudden or repeated change

in their Internet homepage; or their battery has started draining more quickly than it should, they need to know that they should report the problem to IT support immediately.

How to Minimize the Risk of Becoming a Victim of Wire Fraud

If you aren't already aware, attorneys are increasingly being targeted by scammers hoping to get away with wire fraud. Here's just one example of how it can play. An attorney represents a seller in a real estate transaction. Unbeknownst to anyone involved, someone has hacked into and been monitoring the seller's email for a period of time. Once aware that a transaction is about to take place, the hacker uses a spoofed email address of the seller to send new wiring instructions to the attorney in order to have the funds sent to an account the hacker has access to. Attorney fails to catch the altered email address and ends up wiring the proceeds to the wrong bank. So not good.

As an aside, some may wonder what a spoofed email might look like. Although there are a number of ways to spoof email, it can be as simple as this. If an actual email address is Lawfirm@aol.com, a spoofed address might be Lawfirm@aoi.com. If the actual email happens to be Mark.Bassingthwaighte@RECompany.net a spoofed address might read Mark.Bassingthwaite@RECompany.net. Given the busy days we all have; would you catch a subtle change in an email address like the two examples above? Many would not.

If this isn't enough to worry about, there's more. In a recent situation in Virginia a plaintiff attorney's email account was similarly hacked. The hacker sent a spoofed email to this attorney's client. Fortunately, the client questioned the legitimacy of the email, contacted the lawyer who confirmed the email was a fake and the email was deleted. Unfortunately, the plaintiff attorney failed to notify defense counsel that his email account had been hacked. The hacker switched tactics and used a spoofed email to persuade the defense lawyers to wire settlement proceeds to an overseas account. Long story short, a U.S. District Judge basically held the plaintiff's lawyer responsible for the loss due to the lawyer's failure to warn.

Worse yet, the FBI reported that in first three months of 2016 in the U.S. alone over $209 million had been stolen in attacks of this type and the frequency of these attacks continues to rise. Now that I have your attention, the real issue is what in the world can you do to try not become a victim of such attacks? As the title of this post suggests, short of never being responsible for transferring funds of any kind, I'm not aware of any steps that can be taken to make you safe 100% of the time. However, the good news is you can get close.

First, and I know you've heard this before, security basics always play a role. You must avoid the use of free web-based email. If you don't already have a firm website domain, get one and use it to establish your own firm email accounts. Always delete unsolicited email from unknown parties. Never open this spam nor any attachments they may contain. Keep your firewall, operating system and security software current; avoid using unsecured Wi-Fi; and use unique strong passwords (a combination of letters, numbers and symbols) on all accounts and devices. Limit what you post on firm websites and other social media accounts such as information about staff roles and responsibilities and out of office information. Hackers can use this kind of information to determine who to target and when. Most importantly and wherever able, use multi-factor authentication on all email and financial accounts.

Second, establish a policy on wire transfers and couple that with appropriate training of anyone at your firm who may at some point be involved in a wire transfer, to include all attorneys. Initially, the policy should mandate the gathering and verification of contact information from all parties involved at the outset of representation and prohibit the use of any other non-verified contact information during the course of representation. With that in hand, the most important provision of any such policy would be the implementation of a process whereby all wiring instructions are confirmed by use of this previously verified contact information. For example, if wiring instructions initially come via email, use a previously verified number to place a call to the relevant party to confirm the accuracy of the information received. An additional relevant provision might be that all last-minute changes requesting that finds be transferred by a different method or to a different account should be treated as suspect. The request should never be followed until verified by contacting the person purportedly making the request through the use of previously verified contact information. If email security is a concern, another provision might be to require the use of faxes for the exchange of wiring instructions or, better yet, the use of encrypted email or a secure client portal. The absolute best option might be a provision that requires wiring instructions be delivered in person, for example, by the seller at a closing.

Finally, everyone in the firm should be trained to be suspicious and learn how to spot these kinds of scams. Underscore the necessity of remaining vigilant at all times. Training examples that address how these attacks look today might include the following. Look for inconsistencies with email such as various email addresses in use and different spellings of a name. Always carefully check the address of relevant email coming in to make sure it exactly matches the previously verified address in your file. Always question requests for money to be sent to an account that is not in the name of the seller or not in the jurisdiction where the seller is. Be suspicious of requests to wire money when key personnel, such as the attorney in a solo practice, is out of the office or requests that are urgent in nature. And

last but not least, remind everyone that just because the grammar and spelling looks great, that doesn't mean the email is legit. Scammers have spell check too and many of these scammers draft very well written email.

Social Media and the Attorney-Client Privilege Warning

I do believe that as attorneys we all have a pretty good handle on the ins and outs of attorney-client privilege. It's not been an issue for me. What concerns me more is in not knowing how many attorneys know if their clients get it. Stated another way, are you certain that your clients truly understand how easily the attorney-client privilege can be lost or are you running with assumptions? And we all know what they say about running with assumptions.

The reality is that we live and work in a world of instant gratification and instant communication. Why run to the rental store when movies, music, and TV are available online and on demand? By the time a news story is reported on the evening news, it's old news because the story broke on Twitter hours before. Want to share how cute your kids look or the scenic view currently before you while on vacation? Due to the ever-present smart phone, computer tablet, or pocket digital camera, photos and video can be taken and posted for the world to see in a matter of seconds. Just look at the success of Instagram! Our ability to share and consume information on a grand scale has never been greater. Certainly, reasonable minds will disagree as to whether this is a good thing; but that's not the point. My desire is to look at one unintended consequence, which is the ability of clients to lose attorney-client privilege faster and easier than ever.

Is this a problem that lawyers should be concerned about? Absolutely. Clients have already shared what they discussed with their attorney on a variety of social media sites to include Facebook and Twitter. Given that the younger generation seems to have stopped caring about privacy at all I suspect that the frequency of such missteps will only continue to grow. While you can't and shouldn't have to continuously monitor what your clients do online, you must not forget what being in the role of an attorney means. Among other things, it means you're to reasonably consult with clients about the means by which the client's objectives are to be accomplished and you are to explain a matter to the extent reasonably necessary to permit a client to make informed decisions regarding the representation.

Of course, the above is in reference to Rule 1.4 of our Rules of Professional Conduct, which is the rule regarding communication with clients. I view this rule as reminding lawyers of the importance of seeing that their clients are fully informed about all aspects of their matter. This includes making certain that your clients understand how their own

actions or inactions outside of your law office might impact their case. Again, you are the lawyer and your clients expect you to tell them all that they need to know, which in this day and age includes making sure that they don't do stupid when it comes to participating in social media during the course of representation. With this in mind, I offer the following thoughts as a starting point toward bringing this concern into focus for your own practice. You should consider making sure that your clients know the following at a minimum and, of course, there is value in documenting such.

First, remind your clients that there should be no talking about their case with others. Let them know that if they share in a post on Facebook; in an email to a friend; or simply tell a family member, their coworker or neighbor that you said one aspect of their case is particularly weak then their opponent's lawyer could force you and your client to reveal all communications about that aspect of the matter. This could even be worse if your client, be it an individual or entity, actually took a letter, email or other communication to an ad agency, accountant, or financial planner to discuss the ramifications of the advice you have given them. By the same token make certain that your clients understand that a problem is created if you and your client discuss their legal issue in the presence of someone who is not a client in the same matter, be it a friend, parent, or business consultant of some sort. Think this through as discussions are occurring more and more in very nontraditional ways. For example, consider discussions that occur via text message or email. Who might be viewing these? Was anyone blind copied in? It is so easy to hit forward and send to keep the family up to speed on the latest spin in an ongoing divorce saga. These kinds of missteps should not happen and, as the lawyer, it is your responsibility to make certain your clients at least understand the potential fallout if they do these things.

Clearly a simple statement to your client along the lines of "don't talk to others about this legal matter" no longer cuts it. Things your clients post to Facebook or any other social media site can and will be used against them in a court of law and they need to be made fully aware of that reality. One quick aside here, do not try to circumvent the issue by simply encouraging potential or actual clients to close accounts or remove damaging information. I call that spoliation and this can make matters far worse. I have no problem educating clients about how to tighten down privacy settings but this is where it should stop.

Clients should also be told to not use anyone else's computer to communicate with you. A client's work computer (to include a tablet) or company supplied smart phone do not belong to the client and the employing company has the right to monitor communications that occur on its systems. Thus, there should be no emails to and from a work email address and no communications on the work cell phone. Security issues aside, a similar concern arises with the use of public Wi-Fi systems or public computers such as

those found in a hotel or resort business center. When a client is logged on as a guest the terms of service for some of these systems permit monitoring of the communications. Clients should only use private email accounts that are password protected and accessed from their personal smart phones or computers. In addition, make certain that clients do not have shared email accounts or a shared smart phone with a spouse or someone else. If they do, they may need to establish an independent email account that is password protected.

Document these discussions as called for given the specific circumstances in any particular matter. In many situations, this could be accomplished with the use of a social media warning statement in an engagement letter. A sample notice might read as follows:

> We strongly encourage you to refrain from participating in social media (Facebook, Twitter, Tumblr, Flickr, Skype, Instagram, and the like) during the course of representation. Information found on social media websites is not private, can be discoverable, and may be potentially damaging to your interests. Understand that information shared with others be it verbally; in writing via email, text message or letter; or even posted online could lead to the loss of attorney client privilege were that information to relate in any way to the legal matter that we are handling for you. In addition, and without first talking to us, do not attempt to delete any of your social media accounts in an attempt to avoid having anything posted there used against you as doing so can also lead to serious consequences such as sanctions for destroying potentially relevant evidence.
>
> Finally, we also advise you to refrain from communicating with us on any device provided by your employer or any computer, smart phone, or other device that is shared with someone else. In addition, when communicating with us, do not use your work email address or a shared email account. You should only use a private email account that is password protected and only accessed from your personal smart phone or computer.

The use of this what some are now calling "don't do stupid warning" can be useful; but don't rely on this type of notice alone. In the end, it will be client education coupled with periodic monitoring in some circumstances that will make the difference.

Resources

Help in Developing Internet, E-mail & Social Media Use Policies

Let's start with a reminder. The people who use your firm's computers, which includes portable devices such as smart phones or computer tablets, represent a significant risk not only from things like their falling prey to a phishing scam but to intentional misuse. One effective risk management tool that can help address this concern is a well-written online activity policy that is coupled with education and enforcement.

The establishment of rules regarding personal use that address such issues as personal browsing on the Internet, the use of peer-to-peer file sharing networks, personal email accounts, file downloads, and use of social media are of particular importance. Detail ownership and privacy ramifications so that everyone in the firm is aware that they should have no expectation of privacy while using the firm network or any firm provided portable device. You might also consider developing sexual harassment and discrimination policies so that everyone is aware that these rules are in play while online. Underscore the necessity of maintaining a high level of professionalism perhaps by defining inappropriate behaviors via content rules.

Said policies should be set forth in writing and coupled with signed acknowledgement by everyone who will have access to the computer system to include all attorneys at the firm. The policy should include a statement along the lines of failure to comply with the policy will result in discipline that could include termination.

There are a number of resources available that can assist you in developing an online activity policy. The SANS Security Policy Project posts a number of policy templates online that address a variety of important security concerns, many of which you may not have even thought about. These resource materials are available to the public without cost. Topics addressed include an Acceptable Use Policy, a Dial-in Access Policy, an E-mail Policy, a Password Protection Policy, a Remote Access Policy, and a Wireless Communication Policy among many others. The SANS **(S**ysAdmin, **A**udit, **N**etwork, **S**ecurity) Institute is a cooperative research and education organization established in 1989. Over the years, the institute's programs have reached over 165,000 security professionals worldwide. Learn more about the SANS Security Policy Project and access the sample policy language at http://www.sans.org/security-resources/policies/.

A second resource worth reviewing is an article written by Michael Downey entitled "Law Firm Online Activity Policy." This primer is available at

http://www.alacapchap.org/clientuploads/Webinars/2011/webinar0911_SocialNetworking.pdf.

Finally, for a long list of social media policies that a variety of businesses already have in place see http://www.compliancebuilding.com/about/publications/social-media-policies/ or http://socialmediagovernance.com/policies.php#axzz1fmkRy0OX. I strongly recommend taking a look at all of these excellent resources before taking on the task of developing your own policies. While no online activity policy can ensure a 100% risk free environment, a well-drafted and enforced one can certainly go a long way.

Checklist for Becoming Cyber Secure

This checklist is intended to help those who have a desire to become more cyber secure know where to start. It may also be helpful in identifying areas of concern that can and should be discussed with IT support personnel. Most importantly, be aware that cybercrime attack vectors will continue to change and evolve as will the sophistication of the attacks. Becoming cyber secure is an ongoing process, not a once and done effort. That said, here are the basics; and note that when the word "devices" is used, this word is meant to include all mobile devices and any home computers that are being used for work.

____ Keep hardware and software as current as possible. You don't need to be first in line for the latest and greatest; but don't be the last in line either. Newer devices and programs typically include improved security features and cyber criminals often target older devices and programs.

____ Keep your server in a locked room because physical security matters!

____ Deploy effective security software suites on all devices.

____ Deploy effective intrusion detection systems.

____ Deploy a spam filter.

____ Keep all software on all devices up-to-date with the latest critical patches.

____ Determine where all firm data is stored and then create a security policy that responsibly addresses the situation.

____ Password protect all devices.

____ Always use two factor authentication whenever available on any device or with any application.

____ Develop a password policy that mandates the use of strong passwords (12 characters or more) and requires that passwords be changed on a regular basis. Note: Every application and device in use should have its own unique password and no password should ever be reused once changed. The use of a password manager can make this task easier and more secure than, for example, storing passwords in a file labeled "passwords" or writing them down and placing that list in a desk drawer.

____ Prohibit the sharing of user ids and passwords with anyone, to include others within the firm.

____ Have your IT support person change the default values on all wireless routers, server operating systems, etc.

____ Wireless networks should be set up with proper security to include enabling strong encryption. This means you must disable WEP and WPA encryption and require WPA2 encryption. Do not overlook home networks if home computers are being used for work.

____ Backup all data, periodically do a test restore of the backup, and store the backup in accordance with a disaster recovery plan because floods, fires and ransomware attacks happen. Backups should also be encrypted if taken off site or stored in the cloud. If using a cloud vendor, the vendor should not have access to the decryption key.

____ Any device that goes off site and contains any client confidences must be password protected and should be encrypted. This includes jump drives, external hard drives, laptops, smart phones, tablets, and home computers.

____ Limit privileges and access as appropriate. For example, does everyone in the office need access to the firm's financial or employment records? Can everyone download and install anything they want on any device they have access to? Can everyone make changes to the system configuration? Don't make it easy. Place limits on what people can do. Such limits can either be set up electronically via file permissions or physically via a locked door or cabinet.

____ Encrypt email and all data you place in the cloud. Some cloud companies advertise that they encrypt your data but only do so while the data is in transit. You must make certain your data is encrypted "at rest" as well. Better yet, don't rely on the cloud provider for this

at all. Encrypt your data before placing it in the cloud to enable you to have control over the encryption key.

____ Mandate that all work related Internet sessions be encrypted and prohibit the use public computers and unsecured open public Wi-Fi networks. This does mean that access to the office network must always occur through the use of a VPN or some other type of encrypted connection.

____ Prohibit the use of any public computer for any reason. This would include the use of computer stations made available in the business center of a resort or hotel just as one example.

____ Have a policy that prohibits the jailbreaking of any mobile device that will be used for work. Jailbreaking is defined as modifying the operating system from its original state.

____ Never allow a non-employee to have access to your network absent appropriate oversight. In a similar vein, immediately upon the termination of anyone cut off all avenues of access to the network. Terminated individuals should never have access to any office computer or network plug, even if it's to simply download personal files, absent a trusted escort.

____ Provide mandatory social engineering awareness training to everyone at the firm at least once a year.

____ Develop a cyber breach incidence response plan and provide the necessary training. At its most basic, if anyone suspects a device has been breached, teach them how to immediately disconnect from the Internet and/or the office network and instruct them to contact IT support immediately. They should never try to resolve the problem themselves!

____ Purchase a cyber liability insurance policy.

____ Check your internal and Internet-facing network security at least annually to make sure your network is secure. This can be done by having a vulnerability assessment or penetration test done.

____ Properly dispose of any device or digital media that has or had any firm related data on it. Don't overlook digital copiers, digital cameras, memory cards, CDs, DVDs, jump drives, backup tapes, etc. All devices and media must be digitally wiped clean and/or physically destroyed. This does mean that devices cannot be given away for personal use, donated, recycled, or sold unless the entire drives have been overwritten.