In-House Counsel CLE Webinar Series: Grow, Protect, Operate and Finance January 19, 2022

Working Remotely: Legal Ethics & Technology Scams

J.S. "Chris" Christie ©
Dentons Sirote PC
(205) 930-5751
chris.christie@dentons.com

J.S. "Chris" Christie works at Dentons Sirote PC in its Birmingham, Alabama office. The American College of Employee Benefits Counsel selected him as a Fellow in 2015; *The Best Lawyers in America* has listed him since 2005; and *Super Lawyers* named him in 2017 as a Top 50 Attorney in Alabama. He graduated in 1981 from Rhodes College with a B.A. and in 1985 from Duke University with an M.A. and a J.D. From 1985-87, he served as a Peace Corps Volunteer, teaching at the University of Yaoundé School of Law. After 30 years with another firm, he left as of January 1, 2018, to be a candidate for Alabama Attorney General. He frequently speaks and writes on ethics, employee benefits, health care law, and how to try a lawsuit.

TABLE OF CONTENTS

Working Remotely: Legal Ethics and Technology Scams ©

by

J.S. "Chris" Christie [*]

In early 2020, just before the COVID-19 pandemic economic shutdown, the Maze hackers stole and encrypted data of law firms in South Dakota, Oregon and Texas.[1] For just one firm, the hackers demanded a 100 bitcoin ransom to restore the law firm's access to the data and a 100 bitcoin ransom to delete the data instead of selling it – that was a demanded ransom payment total of over $900,000.[2]

What law firm is the next technology scam victim?

I. Legal Ethics and Technology Scams

As discussed below, lawyers have ethical duties of competence, confidentiality and supervision, which require staying abreast of today's ever-changing technology risks. A lawyer should learn and should train his or her staff on cybersecurity to avoid technology related scams, including learn and train on phishing emails, ransomware attacks, and computer system security.

While working remotely, lawyers have the same ethical duties and have increased risks of being a technology scam victim.[3] Computer security may not be as good at home. Increased remote access to computer systems may create increased risks. Lawyers may not be as careful in the less formal settings at home. Lawyers' supervising other lawyers and staff may be more difficult. Attackers should be expected to know about these increased risks and to increase their efforts to scam lawyers.[4]

---

[*] Parts of this paper were published as *What Should an Ethical Lawyer Know about Technology?*, 46(2) *The Brief* 40 (2017).

[1] P. Smith Maze Ransomware Attack Has Hit Small Law Firms in 3 States," https://www.law.com/americanlawyer/2020/02/04/maze-ransomware-attack-has-hit-small-law-firms-in-3-states/ (last visited Dec. 14, 2021).

[2] A. Zmudzinski, "Hackers Stole and Encrypted Data of 5 U.S. Law Firms, Demand 2 Crypto Ransoms," https://cointelegraph.com/news/hackers-stole-and-encrypted-data-of-5-us-law-firms-demand-2-crypto-ransoms (last visited Dec. 14, 2021); D. Olenick, "Maze Ransomware Publicly Shaming Victims into Paying," https://www.scmagazine.com/home/security-news/ransomware/maze-ransomware-publicly-shaming-victims-into-paying/ (last visited Dec. 14, 2021); P. Smith, "Maze Hackers Publish Texas Law Firm's Confidential Data," https://www.law.com/2020/02/11/maze-hackers-delist-texas-law-firm-as-ransom-pressures-mount/ (last visited Dec. 14, 2021).

[3] For some of the federal government warnings about COVID-19 pandemic scams, see https://www.irs.gov/newsroom/taxpayers-should-be-aware-of-coronavirus-related-scams (last visited June 3, 2020); https://www.justice.gov/coronavirus (last visited June 3, 2020); https://www.fcc.gov/covid-scams (last visited June 3, 2020); https://www.fbi.gov/coronavirus (last visited June 3, 2020).

[4] For discussion of lawyers' risks and ethical duties while working remotely, see Penn. Formal Op. 2020-300, "Ethical Obligations for Lawyers Working Remotely," https://www.pabar.org/members/catalogs/Ethics%20Opinions/formal/F2020-300.pdf (last visited June 3, 2020).

As to technology issues, a lawyer should understand the underlying technology risks and the ways those risks can be minimized. At times, a lawyer might consider hiring a cybersecurity consultant, but even knowing when that is appropriate requires some familiarity with the technology issues.

II. ABA Model Rules on Technology and Confidentiality

Why is a lawyer's keeping up with technology to avoid scams an ethical issue? Because lawyers' ethical rules require them to be competent, to safeguard clients' confidential information, and to supervise other lawyers and nonlawyer staff.

1. The Role of the ABA Model Rules of Professional Conduct

To guide lawyers, in light of today's technology and evolving cybersecurity risks, the ABA Model Rules of Professional Conduct were amended in August 2012.[5] The "Technology Amendments" as discussed here are 1.1 (Competence) and Model Rules 1.6 (Confidentiality of Information). In 2017 and 2018, the ABA issued Formal Opinions 483 and 477 as further guidance on lawyers' ethical duties of competence and confidentiality, considering today's technology risks.

In addition to the ethical rules requiring lawyers to be competent and to keep client information confidential, the 2012 Model Rules Technology Amendments inform lawyers' duties to supervise others. Under Model Rule 5.1, partners at law firms and all lawyers supervising other lawyers have a duty to make sure the supervised lawyers follow ethical rules, which includes making sure that supervised lawyers are competent and are keeping client information confidential. Under Model Rule 5.3, all lawyers have a duty to make sure that nonlawyer staff act consistent with the lawyers' duties of competence and confidentiality. In other words, a lawyer not only has duties to learn how to avoid technology risks, but also has duties to ensure that those working for the lawyer also learn to avoid technology risks.

Generally, state ethical rules govern lawyer conduct, not the ABA Model Rules of Professional Conduct. Nonetheless, all states (including California as of November 1, 2018) have adopted a version of the ABA Model Rules. As reflected in the Appendix at the end of this article, twenty-eight states as of February 18, 2020, have adopted all of the 2012 Technology Amendments to Model Rules 1.1 Comment [8], 1.6(c), and 1.6 Comments [18] and [19], twelve states have adopted most but not all of these 2012 Model Rules amendments, and ten states have not adopted any of these 2012 Model Rules amendments.[6]

---

[5] For background on these ABA Model Rules amendments, see the reports of the ABA Commission on Ethics 20/20, filed May 6, 2012 for the ABA Annual Meeting in August 2012. https://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_hod_introdution_and_overview_report.authcheckdam.pdf (last visited Dec. 14, 2021).

[6] Information was not found as to why any state has not already adopted these amendments. A different chart of states that have adopted these amendments as of August 8, 2017, can be found at http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/state_implementat

Whether a state has or has not adopted the 2012 Technology Amendments does not, as a practical matter, significantly change a lawyer's ethical duties to be competent, to safeguard client information, and to supervise those working with the lawyer. Even in states that have not adopted these Technology Amendments, lawyers have ethical duties of competence, confidentiality and supervision, with technology and ethics risks impacting every practicing lawyer. And lawyers' not keeping up with technology might find themselves embarrassed, if not worse.

2. 2021, 2020, 2018 and 2017 Formal Opinions 498, 495, 483 and 477

On March 10, 2021, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 498, recognizing that the "ABA Model Rules of Professional Conduct permit virtual practice, which is technologically enabled law practice beyond the traditional brick-and-mortar law firm."[7] When using technology to practice virtually, "lawyers must particularly consider ethical duties regarding competence, diligence and communication." In addition, a lawyer's duties to supervise subordinate lawyers and staff "requires that lawyers make reasonable efforts to ensure compliance with the Rules of Professionally conduct., specifically regarding virtual practice policies."

On December 16, 2020, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 495,[8] recognizing that technology has allowed lawyers during the COVID-19 pandemic to work remotely and often lawyers have been working in a jurisdiction different from where the lawyer is licensed. ABA Model Rule 5.5(a) prohibits lawyers from engaging in the unauthorized practice of law. The opinion provides guidance that a lawyer may practice while physically in such a different jurisdiction if the lawyer

- does not establish an office or other systematic presence in that local jurisdiction,
- does not "hold out" a presence or availability to perform legal services in that local jurisdiction, and
- does not actually provide legal services for matters in that local jurisdiction, unless otherwise authorized.

On October 17, 2018, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 483,[9] warning as follows:

> Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law

---

ion_selected_e20_20_rules.authcheckdam.pdf (last visited Dec. 14, 2021); *see* https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/chron_adoption_e_20_20_amendments.pdf (chronological adoption by 35 states) (last visited Dec. 14, 2021).

[7] https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba-formal-opinion-498.pdf.

[8] https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba-formal-opinion-495.pdf.

[9] https://www.americanbar.org/content/dam/aba/images/news/formal_op_483.pdf.

> firms are inviting targets for hackers. In one highly publicized incident, hackers infiltrated the computer networks at some of the country's most well-known law firms, likely looking for confidential information to exploit through insider trading schemes. Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.

Opinion 483 explains that the 2012 "Technology Amendments" to Model Rules 1.1 (lawyer competence), 1.6 (lawyers' protecting confidential information), 5.1 (supervisory lawyers' responsibilities for other lawyers) and 5.3 (lawyers' responsibilities for their nonlawyer staff) emphasize that competent lawyers should plan to avoid data breaches and, when a data breach occurs involving material client information, lawyers have a duty to notify clients and take other reasonable steps consistent with the applicable ethical rules.[10]

Formal Opinion 483 expressly built on Formal Opinion 477R, which the ABA Standing Committee on Ethics and Professional Responsibility issued May 22, 2017.[11] Formal Opinion 477R reviews the model ethical rule amendments from 2012 and discusses advances in technology and cybersecurity threats, providing additional guidance as to when lawyers should consider enhanced security measures to protect against the inadvertent or unauthorized disclosure of client information.

3. Model Rules 1.1 Comment [8], 1.6(c), and 1.6 Comments [18] and [19]

As to Model Rule 1.1, the rule already required lawyers to be competent, which requires keeping abreast of changes in the law and practice. The Commission concluded that competent lawyers should be aware of basic technology risks. To emphasize this point, the 2012 Technology Amendments amended Comment [8] of Model Rule 1.1 to add the phrase beginning with *including*: "a lawyer should keep abreast of changes in the law and its practice, ***including the benefits and risks associated with relevant technology*** (emphasis added)." Without the amendment to Comment [8], a lawyer already had a duty to keep up with technology; the amendment emphasizes that duty.[12]

As to Model Rule 1.6, the 2012 Technology Amendments add a new paragraph and change two Comments. The prior Model Rule 1.6 Comments already described a lawyer's ethical duty to take reasonable measures to protect a client's confidential

---

[10] J. Tashea, "ABA ethics opinion offers guidance on data breaches," (October 17, 2018) http://www.abajournal.com/news/article/aba_ethics_opinion_offers_guidance_on_data_breaches (last visited Dec. 14, 2021).

[11]https://www.americanbar.org/content/dam/aba/administrative/law_national_security/ABA%20Formal%20Opinion%20477.authcheckdam.pdf (last visited Dec. 14, 2021); revised and re-issued https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf (last visited Dec. 14, 2021).

[12] *See, e.g.*, ABA Formal Op. 466, Lawyer Reviewing Jurors' Internet Presence at 2 n. 3 (Apr. 24, 2014) (as to whether a lawyer should research a juror's internet presence, saying "we are mindful of the recent addition of Comment [8] to Model Rule 1.1."); Florida Ethics Op. 10-2 (Sept. 24, 2010) ("If a lawyer chooses to use these Devices that contain Storage Media, the lawyer has a duty to keep abreast of changes in technology to the extent that the lawyer can identify potential threats to maintaining confidentiality.").

information from inadvertent or unauthorized disclosures, as well as from unauthorized access. Considering the pervasive use of technology to store and send confidential client information, this pre-existing obligation is now stated explicitly in the black letter of Model Rule 1.6 in the following new paragraph (c): "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."

Comment [18] to new Model Rule 1.6(c) emphasizes that the steps a lawyer ethically should take to reduce risks from technology depends on the circumstances. As Comment [18] explains, a lawyer is not responsible for data breaches "if the lawyer has made reasonable efforts to prevent the access or disclosure." What are the reasonable steps a lawyer should take? Comment [18] indicates as follows:

> 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).

In other words, this Model Rules Comment recognizes that what technology safeguards a lawyer should adopt depends on many factors and requires judgment. As examples, a lawyer should make reasonable efforts to prevent disclosures or access, such as avoiding a lawyer's sending an email to the wrong person, someone's "hacking" into a law firm's network, or staff's posting client information on the internet. As Comment [18] makes clear, not every disclosure is a violation, but reasonable precautions are required.

Before the 2012 Technology Amendments, based on amendments in 2000 quoted in part below, Model Rule 1.6, former Comment [17] and now Comment [19], already described a lawyer's duty when transmitting confidential information:

> This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

In 2000, the "Reporter's Explanation of Changes" for that year's Model Rules amendments included the following explanation for the addition of what was then Model Rule 1.6 Comment [17] and is now Model Rule 1.6 Comment [19]: "Although much of the current debate concerns the use of unencrypted e-mail, the Comment speaks more

generally in terms of special security measures and reasonable expectations of privacy."[13] Again, what safeguards are appropriate when sending client-related confidential information depends on many factors and requires judgment.

To Model Rules 1.6 new Comment [19], the 2012 Technology Amendments added the following new language: "Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these rules." In other words, lawyers should also consider duties arising under HIPAA,[14] Graham-Leach-Bliley ("GLB"),[15] and other laws intended to protect data privacy.

III. Plan to Avoid Being Phished, Especially Being Spear Phished

Ethical lawyers need to be aware of the risks of being phished and plan to avoid being a caught phish. When people say their computer has been hacked, they probably mean an attacker deceived someone into allowing direct access to the computer or into sharing a password, which is often through a phishing email.

1. What is phishing?

Rather than brute force attacks on a computer system, hackers or attackers usually use one of two deceptive methods: (1) sending phishing emails, which urge the email recipient to respond; or (2) using malware that a recipient downloads with games or other apps or downloads by opening infected email attachments, infected thumb drives, or unsafe websites that infect a computer visiting it. Phishing emails appear to be the most common of these two methods.

With a phishing email, the sender is fishing for information to use for whatever purposes the sender can imagine. Spoofing is creating a deceptive phishing email that looks like it is sent by a legitimate business – for example, a bank. Many phishing emails spoof a specific business's emails, often with an email address that looks like the spoofed business's email address.

Spear phishing describes a scam that gathers and uses personal information to urge a targeted individual to respond to emails from what appears to be a trusted source. An eye-opening example of being spear phished can be seen in the underlying facts in

[13] https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/e2k_migated/10_85rem.pdf. (last visited Dec. 14, 2021)

[14] The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, and HIPAA's implementing regulations, 45 C.F.R. §§ 160-64, regulate the collection, use and disclosure of medical information by healthcare providers and their Business Associates (entities that do business with healthcare providers; *i.e.*, lawyers with doctors as clients).

[15] The Gramm-Leach-Bliley Act (also known as the Financial Services Modernization Act), 15 U.S.C. §§ 6801-6827, regulates the collection, use and disclosure of non-public financial information by financial institutions and entities that receive non-public financial information from financial institutions (*i.e.*, lawyers with banks as clients).

Principle Solutions Group, LLC v. Ironshore Indemnity, Inc., 944 F.3d 886 (11th Cir. 2019).

In *Principle Solutions Group*, the court affirmed a summary judgment in favor of the insured that a $1.7 million loss to attackers was covered under a commercial crime insurance policy. *Id*. at 888-89. "The loss stemmed from a sophisticated phishing scheme in which an attacker posing as an executive of Principle Solutions Group, LLC, persuaded [its controller] to wire money to a foreign bank account." *Id*. The insured's controller received an email purporting to be from an executive of the insured about a "secret" acquisition, asking her to wire money "as soon as possible" as instructed by "attorney Mike Leach." *Id*. Then, the controller received an email purporting to be from Leach, a partner at a London law firm. The controller approved the transfer, "but a fraud prevention service, Wells Fargo, asked for verification that the wire transfer was legitimate. [The controller] then confirmed with Leach that [the executive] had approved the transaction. [The controller] relayed this information to Wells Fargo, which released the hold. At 11:21 a.m., about two hours after [the controller] received the first email, [the insured] wired more than $1.7 million to the attackers." *Id*. The controller "discovered that the request was fraudulent a day later when she spoke with [the executive], who told her that he was not even in the office that day. [The executive] promptly called Wells Fargo to report the fraud, but neither [the insured] nor law enforcement could recover the funds." *Id*.

Spear phishing email scams are sophisticated. They use "social engineering," psychologically manipulating people into performing actions or disclosing confidential information.[16] Victims are often motivated by wanting to help. In this context, social engineering might entail the attacker learning enough about a business to pose as the managing executive and send a "spear phishing" email to the business's controller. The underlying facts in the *Principle Solutions Group* case give an example. Essentially the same spear phishing scheme underlies *Medidata Solutions, Inc. v. Federal Insurance Co.*, 268 F. Supp. 3d 471, 473 (S.D. NY 2017), *affirmed*, 729 F. App'x 117 (2d Cir. 2018) (mem.). In *Medidata Solutions, Inc.* a $4,770,226 loss resulted from a wire transfer triggered by an email falsely purporting to be from the insured's President, including a fake "from" field, and related to a secret acquisition and a telephone call from a fake "attorney." In this case, the court granted summary judgment for $5,841,787.37 in damages and interest in favor of the insured.

Another spear phishing email scam seeks to have the recipient change an actual vendor's payment instructions to pay the attacker's bank account instead of paying the vendor. In *American Tooling Center v. Travelers Cas. & Sur. Co. of America*, 895 F.3d 455 (6th Cir. 2018), the appellate court reversed and entered judgment for the insured, ruling that the scam was "computer fraud." A fraudulent email led to the insured's changing an actual vendor's bank account number on payment instructions and then paying about $500,000 of actual invoices to the attacker's bank account. In *Apache Corp. v. Great American Ins. Co.*, 662 F. App'x 252 (5th Cir. 2016), another appellate court

[16] "What is Social Engineering?" https://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering (last visited Dec. 14, 2021).

reached the opposite result, reversing and entering judgment for the insurer, ruling that the scam was not "computer fraud." The insured suffered a $2,400,000 loss caused by changing its actual vendor's bank account number on payment instructions to the attacker's bank account number. The opposite insurance coverage results in these two cases appear to be based on the definitions in the insurance policies. Regardless, a competent lawyer should learn to avoid and should train staff to avoid this type of vendor's payment instructions technology scam.

2. How can a lawyer avoid being a caught phish?

Lawyers can avoid many scams, including phishing scams, with planning. As to phishing emails and malware, a lawyer should decide what steps as technology safeguards are reasonable. Then, the lawyer must not only follow the steps consistently, but also must train his or her staff and make sure they follow the steps too.[17]

To help avoid being caught by a phishing email, what are red flags indicating that an email is risky?

- Purports to be from the IRS, a court, or other government entity
- Purports to be from a financial institution or healthcare provider
- Purports to be from any other intimidating authority or name
- Makes an urgent request with a short deadline like 24 hours
- Insists that transfer of money be kept secret
- Has suspicious or misspelled sender email address or domain
- Has generic, unusual or incorrect name in greeting
- Requests changes in vendor payment instructions
- Requests personal information like account numbers
- Requests clicking on unfamiliar or suspicious URL links
- Offers rewards if click on link or open attachment and reply
- Requests to download a file, especially an .exe file
- Asks for login and password

The red flag of an email's asking for login and password should be the most obvious one. Providing another with one's login and password information is very risky, but replying to an email with that information is just bad – yet people must do it, because phishing emails keep asking for that information.

If a cursor is hovered over (do not click) an email sender's name, the sender's email address and its domain name are shown. Check to see if the email address and its domain name are what one would expect. And sender email addresses can be spoofed. Check to see if the "to" address for a reply (do not send a reply) is the same as the sent address. For an email with links, if a cursor is hovered over (do not click) the link, the link's internet website address (Uniform Resource Locator or "URL") is shown. The

[17] *See generally* Prevent Malware Infection https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/prevent-malware-infection (Dec. 20, 2019) (last visited Dec. 14, 2021)

domain name or the URL should match what one expects. A creative spoofing email might have names that are close to those being spoofed, but with slight differences; for example, "Sirotte" with two ts, rather than "Sirote" with one t. If an email's sender's domain names or link URLs make one suspicious, the email is probably a phishing email.

Avoiding sophisticated scams may require slowing down, researching, and using common sense before acting. A lawyer should consider having technology risks training programs for all who have access, through the lawyer's computer systems, to the internet or to emails. While a cliché, a chain is only as strong as its weakest link. A attacker usually has as much access to a lawyer's computer system through a staff member's responding to a phishing email as when a lawyer does so. In addition to staff training, a lawyer should consider testing to see if his staff is complying with what they have been trained to do. For example, a test phishing email could be sent to see how many staff open a suspicious link or reply to a request for bank account or other personal information.

Another email safeguard is to have a warning, such as "External Email," added as the top line of the message for every email received from an outside sender. The warning should highlight internally any attempt at spoofing the lawyer's own emails, as well as remind the lawyer and his or her staff to be careful.

IV. Plan to Avoid Ransomware Attacks

Ethical lawyers need to be aware of the risks of being a ransomware attack victim. Malware is short for malicious software. It includes computer viruses, worms, trojan horses, ransomware, spyware, and other malicious programs. Today, probably the most serious malware risk is ransomware.[18]

1. What is a ransomware attack?

In a ransomware attack, an attacker uses malware to hold a user's computer usage hostage until a ransom is paid. Ransomware stops one from normally using an infected computer and requires doing something before normal computer use returns. Some ransomware attacks also include threats to disclose private or confidential information. Usually, ransomware requires paying money (a "ransom") to the attacker. Ransomware can encrypt files making them unusable, can prevent access to Windows, or can stop certain apps from working.

[18] Ransomware, Microsoft Malware Protection Center, https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx (last visited Dec. 14, 2021); J. Fruhlinger, "What is Ransomware? How It Works and How to Remove It," CSO (Nov. 13, 2017) https://www.csoonline.com/article/3236183/ransomware/what-is-ransomware-how-it-works-and-how-to-remove-it.html (last visited Dec. 14, 2021).

In June 2019 alone, five health care organizations reported ransomware attacks.[19] Other examples include the WannaCry ransomware that infected 300,000 computers in May 2017 and ransomware attacks that forced DLA Piper to shut down its computers worldwide in June 2017.[20] Cravath and Weils Gotshal are law firms who have been ransomware victims.[21] A September 2016 article reported that two-thirds of ransomware infected companies in the United Kingdom pay ransomware demands, but not all got their data back.[22]

In Alabama, the three hospitals of DCH Health System were impacted by a ransomware attack in the first week of October 2019.[23] According to DCH's website, it discovered the attack October 1, 2019, and immediately implemented emergency procedures, including coordination with law enforcement and engaging independent IT security and forensics experts.[24] The attack shut down DCH's computer systems, forcing it to use paper medical records, to divert non-emergency patients to other hospitals, and to obtain a decryption key from the attacker to restore access to locked systems. In addition, it was reported that calls were made to community members falsely claiming to be from DCH and attempting to obtain personal information.

In addition to these ransomware attack problems DCH described on its website, a class action against the hospital system has been filed. In *Daniels v. DCH Healthcare Authority* (cv-7:19-2086, N.D. Ala., Doc. 1), the plaintiffs allege contract, negligence and breach of fiduciary duty class claims and seek damages and equitable relief. Plaintiffs allege that class members had to forego medical care or had to seek alternative care, and that their identities are now at risk with the data gathered by the attackers.

---

[19] J.Davis, *5 Healthcare Providers Fall Victim to Ransomware Attacks* (June 19, 2019) https://healthitsecurity.com/news/5-more-healthcare-providers-fall-victim-to-ransomware-attacks (last visited Dec. 14, 2021).

[20] J. Tashea & V. Li, "Large Law Firms' Secret Information from Big-money Clients, Entices Cyberthieves," ABA Journal (January 2018) http://www.abajournal.com/magazine/article/large_law_firms_cybertheft_risk (last visited Dec. 14, 2021); DLA Piper, "WannaCry ransomware attack was just the tip of the iceberg," https://www.dlapiper.com/en/uk/insights/publications/2017/06/wannacry-ransomware-attack/ (last visited Dec. 14, 2021).

[21] N. Hong & R. Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL ST. J. (Mar. 29, 2016), https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504 (last visited Dec. 14, 2021).

[22] D. Palmer, "Two-thirds of companies pay ransomware demands: But not everyone gets their data back," http://www.zdnet.com/article/two-thirds-of-companies-pay-ransomware-demands-but-not-everyone-gets-their-data-back/ (last visited Dec. 14, 2021).

[23] https://www.al.com/news/2019/10/dch-health-system-still-grappling-with-ransomware-attack.html (last visited Dec. 14, 2021).

[24] https://www.dchsystem.com/Articles/dch_ongoing_response_to_cyberattack_and_it_system_outage.aspx (Oct. 2-7, 2019) (last visited Dec. 14, 2021).

2. How can a lawyer avoid being a ransomware attack victim?

So, what can a lawyer do to help avoid ransomware attacks? Lawyers should be able to reduce malware risks,[25] including ransomware risks, with the following steps:

- Use strong passwords
- Use multi-factor authentication for remote access
- Install up-to-date antivirus and security software
- Update software, replacing if no longer updated
- Block unsafe, suspicious or fake websites
- Separate work and personal computer use[26]
- Backup important files in a remote, unconnected facility
- Train and test staff on how to avoid ransomware
- Do not open risky emails or email attachments
- Do not click on risky links in emails or websites
- Do not download games or non-work apps
- Do not open risky thumb drives or CDs
- Do not visit unsafe, suspicious or fake websites
- Do not trust telephone caller ID

Once a ransomware or other computer infection is detected, a lawyer should, like any other business, quickly assess what happened, determine what is affected, and contain and limit the damage.[27] A lawyer also should consider communications to clients, courts, and the public. As part of "How do I remove ransomware from my PC," Microsoft offers suggestions for removing some ransomware.[28] The FBI has a publication with many suggestions.[29] If backup data is available, that can provide another alternative after being infected. The FBI used to advise paying the ransom if no other alternatives

[25] "Ransomware groups continue to target healthcare, critical services; here's how to reduce risk," https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/ (last visited May 27, 2020); "Prevent Malware Infection," (Dec. 30, 2019) https://www.microsoft.com/en-us/security/portal/mmpc/shared/prevention.aspx (last visited Dec. 14, 2021).

[26] If separate computers are not possible, at least have separate accounts (especially if a child is using it) on the same computer.

[27] "Troubleshooting problems with detecting and removing malware," https://support.microsoft.com/en-us/help/4466982/windows-10-troubleshoot-problems-with-detecting-and-removing-malware (last visited Dec. 14, 2021).

[28] https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx#faq (Sept. 10, 2019) (last visited Dec. 14, 2021); *see also* J. Fruhlinger, "What is Ransomware? How It Works and How to Remove It," CSO (Dec. 19, 2018) https://www.csoonline.com/article/3236183/ransomware/what-is-ransomware-how-it-works-and-how-to-remove-it.html (last visited Dec. 14, 2021).

[29] https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Dec. 14, 2021).

were available, but as of April 29, 2016, changed its position, and now says do not pay bitcoin ransom to extortionists.[30]

3. What ransomware resources are available?

The Cybersecurity & Infrastructure Security Agency ("CISA")[31] provides numerous resources. For example, on September 30, 2020, CISA released a Ransomware Guide[32] with two parts: Ransomware Prevention Best Practices and Ransomware Response checklist.

V. Plan Other Practical Safeguards

The following gives insights to guide a lawyer's judgment when deciding what steps and safeguards are reasonable to avoid technology scams. In addition to computer system security, to help avoid scams, every lawyer should consider password fundamentals and mobile security.[33]

A. Lawyers and Computer System Security

According to the FBI, today, the three techniques cyber criminals use most often to begin a ransomware attack are email phishing, remote desktop vulnerabilities, and software vulnerabilities, with cyber criminals using "a variety of techniques to infect victim systems with ransomware."[34] Phishing has been discussed above. Both remote desktop vulnerabilities and software vulnerabilities are computer system security issues. Other computer system security issues to consider are encryption and the cloud.

---

[30] https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise (last visited Dec. 14, 2021); "Ransomware Victims Urged to Report Infections to Federal Law Enforcement," FBI's Alert No. 1-091516-PSA, https://www.ic3.gov/media/2016/160915.aspx (last visited Dec. 14, 2021).

[31] https://www.cisa.gov/ (last visited Jan. 8, 2022).

[32] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf (last visited Jan. 8, 2022).

[33] The focus here is on legal ethics and the security of confidential information, without attempting to cover all legal ethics issues arising from new technology. For example, legal ethics and social media is not discussed. Many state advisory ethics opinions address legal ethics and social media, with the ABA Legal Technology Resource Center ("LTRC") gathering resources (last visited Dec. 14, 2021): https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/. Another topic not discussed here is legal ethics and metadata. *See* Ala. Ethics Op. 2007-02 (advising that, without court authorization, a lawyer's mining metadata from an electronic document received from another party is unethical). The ABA has a chart summarizing metadata opinions (last visited Nov. 20, 2018) and described here "Comparison of Metadata Ethics Opinions," https://www.lawtechnologytoday.org/2012/06/comparison-of-metadata-ethics-opinions/ (last visited Dec. 14, 2021), but the chart is unavailable since at least Feb. 19, 2020 (link to chart says "Page Not Found"): http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html.

[34] "High Impact Ransomware Attacks Threaten U.S. Businesses and Organizations," FBI Alert No. 1-1002219-PSA, https://www.ic3.gov/media/2019/191002.aspx (last visited Dec. 14, 2021).

1. What are remote access vulnerabilities?

Remote access to computer systems creates risks, which the FBI calls vulnerabilities. But lawyers want to access their computer systems from home or wherever, with a laptop or other device. The computer system risks include brute force methods, which is a hacker's using trial and error to obtain user IDs and passwords. But phishing emails and other deceptive methods, which can allow direct access to the computer system, are bigger risks. In 2016, PhishMe reported that 93% of phishing emails were related to ransomware.[35]

Lawyers should consider a robust network system of rules to follow before allowing users to access a computer over the internet. Issues to consider include the strength of passwords required (discussed below), two factor identification, and limiting what can be accessed remotely. Lawyers also should consider hiring a computer security consultant to evaluate their network's security.

When identifying parts of a computer system to safeguard, a lawyer should consider not only servers, desktops, and laptops, but also tablets, smart phones, copiers, scanners, and any other device that can connect to a computer system or can download data or can access the internet. A computer system can limit what access a remote device or what access an individual user might have. For example, Microsoft offers "controlled folder access" to protect against threats such as ransomware.[36] Particularly for administrator accounts, use should be restricted to when using such an account is necessary and only non-administrator accounts should be used to check email or browse the internet.[37]

Access to computer systems through IoT (Internet of Things) devices is expected to become a bigger risk. In lawyers' offices, not only printers and copiers can be connected to the internet, but also thermostats and even lights. IoT devices can be protected through strong passwords, isolating IoT devices from other computer systems, and other means.[38]

For heightened security, a lawyer might consider multi-factor identification to access a lawyer's email or any computer system. Two-factor identification can require a password and other information. For example, logging on can require a password that, when entered, places a call to the user's cell phone, with access allowed only if the cell phone is answered. Another example, access might require a password and a thumbprint.

---

[35] http://phishme.com/q1-2016-sees-93-phishing-emails-contain-ransomware/ (last visited Dec. 14, 2021).

[36] "Protect important folders with controlled folder access," https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/controlled-folders (Aug. 4, 2019) (last visited Dec. 14, 2021).

[37] "Prevent Malware Infection," https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/prevent-malware-infection (Dec. 30, 2019) (last visited Dec. 14, 2021).

[38] J. Lerner, "IoT Security: 5 Tips to Protect Your Devices from Hackers," (Nov. 20, 2018) https://www.enterprisemobilityexchange.com/eme-security/news/iot-security-issues-devices (not available as of Dec. 14, 2021) (last visited Dec. 14, 2021).

In addition, a lawyer should consider what steps to take when an employee leaves. When staff changes, unused user accounts should be terminated, passwords changed, and other steps considered.[39]

2. What are software vulnerabilities?

A attacker or hacker can gain computer access by taking advantage of computer systems' software vulnerabilities. A lawyer should make sure that his or her computer system has updated antivirus software and other security software, including a firewall. The specifics on programs as safeguards to protect entire computer systems may require a consultant. Unless one is the rare lawyer with the technical skills, finding someone with expertise to help is advisable.

A lawyer should consider regularly updating software and replacing software that is no longer being updated. For example, because Microsoft no longer supports Windows XP, it no longer has security updates. Windows XP still operates but becomes more and more vulnerable to security risks and malware infections as time passes.

3. Should a lawyer encrypt data?

Despite technology risks, most law firms report they do not use encryption.[40] For all electronic data (*i.e.*, information), a lawyer should consider whether the data should be encrypted. Encryption is the process of encoding data so attackers cannot read it, but authorized parties can. Encryption turns words into scrambled gibberish. Many modern encryption programs use factoring and prime numbers. A prime number can only be divided by one and itself. Factoring is identifying the prime numbers multiplied together that result in a number. Encryption today can make it very difficult for computers to decipher encrypted data without the key.

A lawyer should consider what data might need to be encrypted. ABA Formal Op. 477R, p. 5, warns that "it is not always reasonable to rely on the use of unencrypted email."[41] As discussed below, some email programs automatically encrypt data when sent.

Another issue is whether to encrypt data at rest. Such encryption complicates the user experience; encrypting all electronic information interferes with using the information efficiently. Data shipped or otherwise taken out of the office creates

---

[39] M. McGee, Mitigating Threats Posed by Terminated Employees, Data Breach Today, (Dec. 1, 2017) https://www.databreachtoday.com/mitigating-threats-posed-by-terminated-employees-a-10503 (last visited Dec. 14, 2021); "Insider Threats and Termination Procedures, U.S. Dept. HHS (Nov. 2017) https://www.hhs.gov/sites/default/files/november-cybersecurity-newsletter-11292017.pdf?language=es (last visited Dec. 14, 2021).

[40] D. Ries, "Security," ABA TechReport 2017 (last visited Dec. 14, 2021) https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security.html.

[41] https://www.americanbar.org/content/dam/aba/administrative/law_national_security/ABA%20Formal%20Opinion%20477.authcheckdam.pdf (last visited Dec. 14, 2021); https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf (last visited Dec. 14, 2021).

additional risks. If data relating to the representation of a client is on a portable hard drive, a thumb drive, a mobile device, or attached to an email, whether it should be encrypted requires more thought and depends on several factors. Many free encryption tools are available.[42]

4. Should a lawyer use the Cloud?

Another risk is using the cloud. First, this cloud has nothing to do with weather. Years ago, when engineers were diagramming computer networks, they did not know how to represent the internet, so they just drew a cloud. Today, "the cloud" means a computer accessible through the internet. While working remotely, cloud issues become more likely.

If a lawyer is using the cloud, the lawyer stores data on a computer owned by a third party. Cloud services are hosted by Amazon, Microsoft or another cloud data center provider.[43] A firm could host and provide its own private cloud services, but a vendor for at least some aspect of using the cloud is highly likely. Because cloud computing places client data on remote servers not usually in a lawyer's direct control, whether lawyers should use the cloud is a question.[44]

Often, using a cloud vendor is more secure than what a lawyer might be able to have on the lawyer's own computer systems. A cloud vendor is also likely to have better backup capability. If considering a cloud vendor, a lawyer might include asking or investigating the following questions:

- How does the vendor safeguard data?
- How often does the vendor backup data?
- Does the vendor backup data in multiple locations?
- Does the vendor have experience with a ransomware attack recovery?
- How stable is the vendor as a business entity?
- Does accessing the lawyer's data require proprietary software?
- If the relationship ends, how is the data accessed and returned?
- After data is deleted, can the vendor certify that it is destroyed?
- Are the vendor's safeguards HIPAA and GLB compliant?
- What confidentiality provisions are in the vendor's standard contract?
- Will the vendor agree to other confidentiality provisions?

---

[42] http://www.gfi.com/blog/the-top-24-free-tools-for-data-encryption/ (last visited Dec. 14, 2021).

[43] D. Kennedy, "2019 Cloud Computing," TechReport 2019, Oct. 2, 2019 https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/cloudcomputing2019/ (last visited Dec. 14, 2021).

[44] *See* "Vendor Contracting Project: Cybersecurity Checklist," ABA Cybersecurity Legal Task Force (April 13, 2017) https://www.americanbar.org/content/dam/aba/administrative/law_national_security/cyber-task-force-vendor-contracting.pdf (last visited Dec. 14, 2021).

In summary, when choosing a cloud vendor, a lawyer should consider whether the data will be secure and backed-up and whether he or she will have any problems if his or her relationship with the vendor might end.

5. Should a lawyer have cyber security insurance?

One lesson for lawyers from the *Principle Solutions Group* and other cases discussed above is that Cyber Liability Insurance is available and can cover cyber losses, but might not. Whether a lawyer should have Cybersecurity Insurance depends on many factors.[45] It can be expensive. And having Cybersecurity Insurance can involve negative tradeoffs: For examples, losing control of negotiations, delays, and attackers learning coverage limits and deductibles and using those to increase demands.

6. Should a lawyer have an Incident Response Plan?

Lawyers need to have an Incidence Response Plan, because security incidents and data breaches may occur no matter how careful.[46] The plan should be appropriate for the size of the firm and the sensitivity of data. For example, a solo practitioner with data that could be used to make money from buying or selling stocks needs to consider the motives others will have to access that data. All lawyers and staff should have some Plan training. The Plan should not depend on one person, because he or she might be inaccessible when disaster strikes. And the Plan should be accessible if the computer system is not.

7. Miscellaneous Computer System issues

A lawyer should emphasize to all working with him or her, and to clients, not to have client related or other confidential conversations in places where the conversations can be overheard. This risk is increased while working remotely.

A lawyer should avoid having Amazon Alexa or Google voice assistants where client-related or other confidential conversations occur. These devises record and store voices, even when one might think they are turned off. For lawyers and staff working remotely, this risk is one more likely than others to be overlooked.

A lawyer should consider regular automatic backups of computer systems. In anticipation of ransomware attacks, as well as natural disasters, a lawyer should also consider having such backups in more than one location and at least one remote geographically from the main computer systems. In addition, at least one of the backup systems should normally be separate from and not connected to the main systems.

---

[45] P. Hans, "Cyberattacks—A Spotlight on Ransome Losses and Insurance" (Sept. 10, 2021) https://www.americanbar.org/groups/litigation/committees/insurance-coverage/articles/2021/cyberattacks-ransom-losses-insurance/ (last visited Jan. 8, 2022); P. Prakash, "What is Cyber Liability Insurance, and Do You Need It?" (Oct. 25, 2019) https://www.fundera.com/blog/cyber-liability-insurance (last visited Dec. 14, 2021).

[46] *See* D. Nelson, D. Ries & J. Simek, *What to do When Your Data is Breached*, Mich. B.J. 54 (Sept. 2018) http://www.michbar.org/file/barjournal/article/documents/pdf4article3480.pdf (last visited Dec. 14, 2021).

A lawyer should consider whether his or her safeguards are HIPAA and GLB compliant. Even if the lawyer does not represent healthcare providers or financial institutions, he or she is likely to have medical and financial information that raises the same or similar confidentiality issues. One might also argue that all confidential information, including attorney-client communications, should be protected with the same or similar safeguards.

Another computer system consideration might be what to do with computers when they are no longer being used. Lawyers should be careful when discarding computers, copiers, and any other devices storing data. A possible risk that might be missed is data on leased computers and copiers. Note that Affinity Health Plan, Inc., paid a fine of $1,215,780 for alleged HIPAA violations after it returned multiple copiers to a leasing agent without erasing data on the copiers' hard drives.[47]

B. Lawyers and Videoconferencing

For most purposes, a lawyer should be comfortable with videoconferencing, assuming appropriate safeguards are used. As the COVID-19 pandemic shutdown began, Zoom's videoconferencing received negative publicity. One Congressperson demanded that the United States House of Representatives stopped using Zoom.[48] Apparently, the Congressperson misunderstood what had happened during a Zoom meeting.[49] And Zoom has addressed some security issues since then.[50]

As with any other computer communications, videoconferencing requires safeguards.[51] Steps to consider include requiring a password to join a meeting, not sending links or passwords until after registration, asking registrants not to share links and passwords, setting up a waiting room where a gatekeeper must allow individuals to join the meeting, and have someone manage muting, video and screen sharing options.[52]

C. Lawyers and Password Fundamentals

Every lawyer should consider password fundamentals for protecting confidential information. Good passwords are a simple safeguard to protect client information.

---

[47] http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/health-plan-photocopier-breach-case/index.html (last visited Dec. 14, 2021).
[48] https://jordan.house.gov/news/documentsingle.aspx?DocumentID=399178 (last visited June 3, 2020).
[49] https://thehill.com/homenews/house/492245-jordan-calls-for-oversight-to-stop-conducting-business-via-zoom (last visited June 3, 2020).
[50] https://zoom.us/docs/en-us/privacy-and-security.html?zcid=3736&creative=430738469005&keyword=%2Bzoom%20%2Bsecurity&matchtype=b&network=g&device=c&gclid=Cj0KCQjwlN32BRCCARIsADZ-J4uyyz4ROKHSV0Bl0LlRbmPni0P8DzCSaBSdmRoPoWQaqHmBCF_zRMYaAti8EALw_wcB https://explore.zoom.us/docs/doc/Zoom-Security-White-Paper.pdf (last visited Dec. 14, 2021).
[51] Penn. Formal Op. 2020-300 at 12, "Ethical Obligations for Lawyers Working Remotely," https://www.pabar.org/members/catalogs/Ethics%20Opinions/formal/F2020-300.pdf (last visited June 3, 2020).
[52] *Id.*

A lawyer's strong passwords can sometimes interfere with the lawyer's efficiently using a computer. A password needs to be remembered, but easy passwords can create risks. Hiding a password under the telephone may not be as bad as putting it on a post-it note on the computer screen, but an unauthorized person wanting to access a computer might look around for passwords written down. Moreover, using the same password for every purpose or not changing passwords periodically can increase risk.

In addition, some sites have password prompt questions such as "What is your mother's maiden name?" If security matters, using a prompt that a attacker can research and discover creates a risk.

What are bad (weak) passwords? In 2021, NordPass released its annual most used and thus worst passwords list. Topping the list was "123456," followed by the slightly more inventive "123456789;" next were "qwerty" and "password."[53] Any password that an attacker could guess is a bad password.

Good (strong) passwords include uppercase and lowercase letters, numbers, symbols, and spaces. For many purposes, an eight-digit password with some combination of several types of these characters should be plenty strong.

An easy way to remember good passwords is to use leetspeak (or l33t$peak). With l33t$p3ak, one replaces letters with other characters. For example, password can become P@55w0rD.

The longer a password is, the harder it is to crack. Not only are passwords with characters that are not letters and numbers difficult to guess, but programs that try every possible password (brute-force attacks) have great difficulty breaking long passwords using different types of characters.

Even stronger passwords combine l33t$p3ak with phrases ("passphrases"). More than 15 characters can currently make a passphrase too difficult to crack for almost any attacker. For example, M0unt@in M@n 1234 5treet is not impossible to remember but would be much harder to hack than any eight-character password.

Applications called password managers are available. One service is called LastPass. It helps generate secure passwords and helps the user remember them. Using this type of tool, however, is difficult to manage for a law firm network and might create a risk of a attacker's breaking into the service and then having all the lawyer's passwords.

Like other safeguards, good passwords are for all who access the lawyer's computer systems. A lawyer should require staff to have good password fundamentals, train staff on those password fundamentals, and find ways to ensure staff compliance with good password fundamentals.

---

[53] For 2022's worst passwords, see https://cybernews.com/best-password-managers/most-common-passwords/ (last visited Jan. 8, 2022). For a list of 2019's worst passwords, see https://www.teamsid.com/1-50-worst-passwords-2019/ (last visited Dec. 14, 2021).

D. Lawyers and Mobile Security

Among the mobile device security risks are losing computers that are mobile devices (laptops, tablets, smart phones) and Wi-Fi interception. Among the risk-reducers might be strong passwords, remote wiping, encryption, two-factor identification, inactivity timeouts, authorization before downloading applications, and automatic wiping if access is attempted incorrectly a certain number of times.[54]

1. Mobile Security for Lawyers

Years ago, many law firms only allowed firm approved and owned mobile devices (usually BlackBerry smartphones). A September 2013 article in the *ABA Journal* called BYOD (Bring Your Own Device) "a nightmare" from a security perspective and quoted a security firm executive as follows: "We strongly believe that lawyers should connect to law firm networks only with devices owned and issued by the law firms."[55] With advances in smartphones and tablets, however, BYOD has become the accepted norm.

The initial concern is easy to understand. Imagine a lawyer's leaving a smartphone at a bar. What client information is on the smartphone in email, email attachments, or accessed documents? What access to the firm email system or other systems can a attacker find through the smartphone? How long before the law firm learns that its drinking lawyer lost his smartphone?

For any mobile device that has information relating to the representation of a client, a lawyer should at least consider having a six-digit PIN and should consider having a stronger password. For smartphones with a swipe pattern as the password, a lawyer might consider changing the password periodically to avoid a wear pattern on the screen. A lawyer might also consider remote wiping and other risk-reducing steps.

For any mobile device that has information relating to the representation of a client, a lawyer should consider having all possibly confidential data encrypted. Laptops, tablets and smartphones can be stolen, regardless of how careful a lawyer tries to be.

Lawyers might consider Mobile Device Management (MDM) software, which can secure, monitor, and support all connected mobile devices.[56] Through a remote MDM console, using commands sent over the air, an administrator can update any mobile

---

[54] H. Dowden, "The 7 Mobile Device Security Best Practices Y9u Should Know for 2022," (Dec. 8, 2021) https://www.ntiva.com/blog/top-7-mobile-device-security-best-practices (last visited Dec. 14, 2021).

[55] J. Dysart, "New hacker technology threatens lawyers' mobile devices," Sept. 1, 2013, http://www.abajournal.com/magazine/article/new_hacker_technology_threatens_lawyers_mobile_devices (last visited Dec. 14, 2021). Since 2013, employers have generally adapted to BYOD. "BYOD Policies: What Employers Need to Know," https://www.shrm.org/hr-today/news/hr-magazine/pages/0216-byod-policies.aspx (Feb. 1, 2016) (last visited Dec. 14, 2021); M. Dhingra, "Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)," http://www.sciencedirect.com/science/article/pii/S1877050916000326 (last visited Dec. 14, 2021).

[56] To view Citrix's MDM video, see https://www.youtube.com/watch?v=oUYYZdSXQTQ (last visited Dec. 14, 2021).

device or group of mobile devices. MDM can separate email and associated content away from applications; can distribute applications, data, and configurations; and can even be used to deploy securely new applications from a law firm's "app store." MDM can also remote-wipe the mobile device.

For a mobile device used for work, a lawyer should consider what software (applications) are downloaded, because some might compromise the device. If a child plays with a work mobile device, a lawyer should consider the risks of the child's deleting documents, sending documents to the wrong people, or downloading malware.

For simpler mobile device security, instead of (or in addition to) the above considerations, a lawyer might manage risks by not having or limiting the confidential information on the device. A mobile device that only has the two most recent weeks of confidential client information does not pose the same risks as a mobile device with thousands of emails with confidential client information in the text of the emails.

2. Wi-Fi Interception and Security for Lawyers

If a lawyer uses public Wi-Fi, especially in a café or hotel hot spot, a attacker could theoretically intercept what is sent, sometimes called "packet sniffing." Packet sniffing captures packets of information sent through the air between the device and the hot spot. These packets can be passwords, emails, or whatever is sent. Software to packet-sniff (a packet analyzer) is readily available. Wireshark sells packet capture devices.[57]

Packets can be sent as "clear text" (unencrypted), which means anyone can read them as plain English, or packets can be sent on an encrypted connection, which means even though people can intercept them, they cannot read them. If a lawyer uses Microsoft Exchange and has encrypted connections, the lawyer should not have an unencrypted email interception problem, because the emails are encrypted during transmission.

If a lawyer uses a general webmail service like normal Gmail, the lawyer might be sending clear text and have an avoidable risk.[58] On the other hand, a lawyer can have a Gmail account that is secure. In the website address header (the URL for uniform resource locator), look for an S after the HTTP. In other words, "HTTPS:" in the URL indicates that the site uses encryption.

When using Wi-Fi, an alternative to using an encrypted email system might be to use a VPN connection to a firm network. A VPN connection provides a secure tunnel that funnels web activity, encrypted, through the secure connection. This connection is a secure way to work on Wi-Fi. A lawyer's email system can require a VPN connection to connect to email.

---

[57] https://www.wireshark.org/ (last visited Dec. 14, 2021).

[58] For a general discussion of lawyers' communicating confidential information by email and risks lawyers should consider, see Texas State Bar Op. No. 648 (2015), http://www.legalethicstexas.com/Ethics-Resources/Opinions/Opinion-648.aspx (last visited Dec. 14, 2021).

VI. Conclusion

As the Model Rules' 2012 Technology Amendments and the ABA's 2017 Formal Opinion 477R and 2018 Formal Opinion 483 emphasize, an ethical lawyer should have reasonable technological competence to avoid technology scams. A lawyer should use good judgment, taking reasonable steps to reduce technology risks and to safeguard information. And a lawyer should not only consistently safeguard confidential data but should also train his or her own staff to do the same.

APPENDIX

State Actions on ABA's 2012 Technology Amendments for Model Rules 1.1 Comment 8, 1.6(c), and 1.6 Comments 18 and 19[i]

State	Amended Model Rule 1.1 Comment [8]	Amended Model Rule 1.6(c)	Amended Model Rule 1.6(c) Comment [18]	Amended Model Rule 1.6(c) Comment [19]
Alabama	No	No	No	No
Alaska	Adopted, no Comment numbers	Adopted with language from Comments	Adopted, no Comment numbers	Adopted, no Comment numbers
Arizona	Adopted as Comment [6]	Adopted as Rule 1.6(e)	Adopted as Comment [22]	Adopted as Comment [23]
Arkansas	Adopted	Adopted	Adopted	Adopted
California	No	No	No	No
Colorado	Adopted	Adopted	Adopted	Adopted
Connecticut	Adopted, no Comment numbers	Adopted as Rule 1.6(e)	Adopted, no Comment numbers	Adopted, no Comment numbers
Delaware	Adopted	Adopted	Adopted	Adopted
District of Columbia	Adopted as Comment [6]	No	No	Adopted as Comment [40]
Florida	Adopted, no Comment numbers	Adopted as Rule 1.6(e)	Adopted, no Comment numbers	Adopted, no Comment numbers
Georgia	No	No	No	No
Hawaii	No	No	No	No
Indiana	Adopted as Comment [6]	No	No	No
Illinois	Adopted	Adopted as Rule 1.6(e)	Adopted	Adopted

Iowa	Adopted	Adopted as Rule 1.6(d)	Adopted sentence	Adopted
Kansas	Adopted	Adopted	Adopted as Comment [26]	Adopted as Comment [27]
Kentucky	Adopted as Comment [6]	No	No	No
Louisiana	Adopted	Adopted	Adopted	Adopted
Maine	No	No	No	No
Maryland	No	No	No	No
Massachusetts	Adopted	Adopted	Adopted	Adopted
Michigan	Adopted similar language, no Comment numbers	No	No	No
Minnesota	Adopted	Adopted	Adopted as Comment [17]	Adopted as Comment [18]
Mississippi	No	No	No	No
Missouri	Adopted as Comment [6]	Adopted	Adopted as Comment [15]	Adopted as Comment [16]
Montana	No (no Comments)	Adopted	No (no Comments)	No (no Comments)
Nebraska	Adopted as Comment [6]	No	No	No
Nevada	No (no Comments)	Adopted	No (no Comments)	No (no Comments)
New Hampshire	Adopted similar language	Adopted	Adopted	Adopted
New Jersey	No	Adopted as Rule 1.6(f)	Adopted, no Comment numbers	Adopted, no Comment numbers

New Mexico	Adopted	Adopted	Adopted as Comment [20]	Adopted as Comment [21]
New York	Adopted with different language	Adopted with different language	Adopted with different language as Comment [16]	Adopted with different language as Comment [17]
North Carolina	Adopted	Adopted	Adopted as Comment [19]	Adopted as Comment [20]
North Dakota	Adopted as Comment [5]	Adopted as Rule 1.6(d)	Adopted	No
Ohio	Adopted	Adopted	Adopted	Adopted
Oklahoma	Adopted as Comment [6]	Adopted	Adopted as Comment [16]	Adopted as Comment [17]
Oregon	No (no comments(	Adopted	No (no comments)	No (no comments)
Pennsylvania	Adopted	Adopted as Rule 1.6(d)	Adopted as Comment [25]	Adopted as Comment [26]
Rhode Island	No	No	No	No
South Carolina	Adopted as Comment [6] with added language	Adopted	Adopted as Comment [20]	Adopted as Comment [21]
South Dakota	No (no comments)	Adopted	No (no comments)	No (no comments)
Tennessee	Adopted	Adopted as Rule 1.6(d)	Adopted	Adopted
Texas	Adopted with added language	No	No	No
Utah	Adopted	Adopted	Adopted	Adopted
Vermont	No	No	No	No
Virginia	No	No	No	No

Washington	Adopted	Adopted	Adopted	Adopted
West Virginia	Adopted	Adopted	Adopted	Adopted
Wisconsin	Adopted	Adopted as Rule 1.6(d)	Adopted	Adopted
Wyoming	Adopted as Comment [6]	Adopted	Adopted	Adopted

[i] As of February 22, 2020. Thank you to R.M. English for his help with the Appendix.