ARTICLE FOR CLE CREDIT

Cyber Security Tools & Techniques: How to Meet Your Ethical Obligations

BY JOEL G. SELIK, ESQ.

PHOTO CREDIT: SHUTTERSTOCK.COM

Attorneys are required by the Nevada Rules of Professional Conduct (RPCs) to have a working knowledge of cybersecurity and to prevent disclosure of client information. See, e.g., ABA Formal Opinion 477R (2017).

These duties arise from attorneys' basic ethical duties to protect client confidences, RPC 1.6, and the duty of competence, RPC 1.1. These duties, combined with electronic data being ubiquitous in the modern practice of law, require us:

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. [Model Rules of Prof'l Conduct 1.1, Comment 8].

It is no longer acceptable for attorneys to claim to be Luddites and refuse to learn about electronic data, risks, tools, and issues.

Several ABA Formal Ethics Opinions have identified attorneys' duties as to securing electronically stored and transmitted client information, (Opinion 477R, 2017), duties attorneys have to prevent a cyber-breach and what to do once there has been a breach (id. and Opinion 483, 2018), and issues surrounding lawyers working remotely (Opinion 495, December 2020).

Attorneys have a duty to understand where client information is vulnerable to unauthorized access. Any client data that is kept in the cloud or transmitted over the internet, wi-fi, or email is vulnerable. Further, attorneys have a duty to understand the various security measures that are available and determine how to best protect their

clients' information. Attorneys also have duties to: monitor cyber-breaches, supervise lawyer and non-lawyer staff to make sure they are not allowing unauthorized access to client information, and to vet vendors who have access to cyber-data.

Tools and Techniques for Cybersecurity

Secure Passwords

A strong password is considered the most important security you can have. A strong password consists of incorporating all of the following, random capital letters, random lowercase letters, numbers, and special characters (e.g., !, @, #, _). Experts advise not to use real words when using letters. One method of creating passwords is to use the first five letters of each word of a favorite song; use personally significant numbers from your past (do not use numbers that are currently significant such your address, telephone number, birth date, anniversary, etc.), and certain special characters in specific locations in each password.

Experts further advise using a different password for each website or vendor; you can use a standard secure password changed only slightly for separate websites. Experts are now advising that, more important than changing passwords regularly, is having a complex secure password.

Remember, we also have a duty to make certain that all attorneys and non-attorneys that we supervise also have secure passwords.

Password Managers

There are programs available called password managers that allow you to have extremely complex passwords without having to remember each password. You only have to remember the one complex password for the password manager. These programs are inexpensive.

Two-Step Verification

In addition to passwords, many websites and vendors offer two-step verification. This type of security requires the user to sign-in using a username and password, and then a code is sent to an email address or via text. Using two-step verification takes additional time to access the website and data, and the additional steps will slow down your work. Considering the effect on your work, i.e., the ability to effectively represent your clients, is one of the factors that is a proper consideration in determining what security measures to take. See Comment 18 to Model Rule of Professional Conduct 1.6(c) and ABA Formal Opinion 477R (2017). Attorneys must weigh the burdens and protections each method of security may provide.

Updating Software

In addition to strong passwords, updating programs is critical for cyber-security. All programs, including operating systems (OS), need to be updated regularly. As new security holes are found in software and new viruses found, software manufacturers update their software, sometimes as often as several times a week. For example, Microsoft constantly adds patches and updates to Windows OS that are critical for cybersecurity. Another example is Zoom, which updates their software constantly. Many programs allow automatic updating—attorneys should regularly check on software to confirm it is being updated.

Wi-fi routers are easy to forget. Attorneys should make certain that the wi-fi passwords are secure and the firmware is regularly updated.

Anti-Virus

For several decades, anti-virus programs have been the basic, first-line defense, to protecting computers and electronic data. There are many different programs, including high-quality free programs; even the best programs are inexpensive. It is not going out on a limb to state that failure to use a good, current, anti-virus program violates an attorney's ethical duties.

CONTINUED ON PAGE 20

CONTINUED FROM PAGE 19

Cybersecurity Tools & Techniques

VPN

A Virtual Private Network (VPN) connects to your computer, not through the computer's usual internet protocol (IP) address, but through a disguised IP address. This creates a "tunnel" for the information going over the internet creating additional security. Be aware that using a VPN will likely require additional clicks to prove you are not a robot and turning the VPN off and on to get to some websites.

You can use a VPN anytime you connect to the internet, but it is especially crucial if you ever connect to public wi-fi, such as at coffee shops or hotels.

Another trick hackers use is, where there is public wi-fi, to add a spoofed public wi-fi to get you to connect through their system. For example, if you are at Joe's Coffee, their public internet might be "JoesPublic." The hacker can create another public wi-fi and call it "JoesCoffeePublic." Make certain that you are connecting to the official wi-fi and that you are using a VPN.

Staff

As attorneys are responsible for their attorney and non-attorney staff, (RPCs 5.1 and 5.3), attorneys must make certain they are also complying with cybersecurity, including using safe passwords and not succumbing to phishing. This process may require reviewing staff passwords and testing for failing for phishing emails.

Encrypted Email

Anytime an attorney sends client data, either within an email, or attached to an email, the attorney must consider the risk if that data was hacked. Basic email is not, generally, encrypted. This means that if the email is intercepted anywhere along the way, the data is available to the interceptor. Data can be sent more securely by using encrypted email (although even with encrypted email, the attachments may not be encrypted), using a secure file-sharing program such as Snyc.com, Dropbox, OneDrive, Google Drive, Box, Apple iCloud, etc., or by separately encrypting the attachment.

Many email programs are either encrypted by default or have features allowing encryption. There are other services that fully encrypt all emails.

Except for data that may be particularly sensitive, such as medical information or trade secrets, attorneys are not currently required to use encrypted email. ABA Formal Opinion 99-413 held that hacking of email is a crime; just as with regular paper mail, attorneys have a reasonable expectation of privacy in their emails. As hacking continues to grow and as programs to protect emails improve and become easier to use, encrypted email will become the standard of care.

Encrypted Computers

For the most part, the data kept on attorneys' computers is not encrypted. This means that anyone who can access the data, such as with a USB drive ("thumb" or external drive) or by hacking, can easily steal that data. For a home or office computer that is protected by a good anti-virus program, highly secure passwords, strongly secure wi-fi, and a locked building, encryption may not be necessary. But, for portable devices, such as a mobile phone or laptop, there is a much higher risk of hacking or direct access to the data if the device is lost or stolen. If you take data out of the office, whether it be on a cell phone, USB drive, CD-ROM, or laptop, encrypting the data should be considered.

Travel Tip

If you travel on an airplane, laptops and cellphones are subject to access by

governmental authorities. Encryption and passwords are not enough to protect your client data as governments can compel access. Therefore, it may be prudent to remove all client and other confidential information from the computer before travelling and download the needed information upon arrival at your destination. This goal can be easily and quickly accomplished with cloud-based practice management software or cloud-storage programs.

Alexa, Google Home, Siri

These smart home devices use voice commands without the need to turn anything on or push a button. Some televisions and remote controls can have smart home features built in. The devices are always listening (or can be). This situation allows the devices to listen to everything that is said, and this information is then available to the provider (e.g., Amazon or Apple). If an attorney is in a room with a device that is always listening, and client matters are discussed or there are client telephone conversations, this is an ethical violation.

Online Vendors

Any company that an attorney uses that may provide, use, and receive client confidential information must be vetted to make certain that they are properly protecting the clients' data.

Messaging

There are instant messaging apps, such as text messaging, Facebook Messenger, WhatsApp, and case management software messaging systems. If you send client data or discuss cases, determine the level of security that each has (Facebook Messenger is not encrypted, WhatsApp is).

Label Documents

One step that the ethics opinions discuss is labelling documents as confidential. While this does not prevent hackers from accessing the data, if there is unauthorized inadvertent access, this could help maintain client confidentiality.

Attorneys are ethically obligated to attend to cybersecurity. It is impossible for the average attorney to know everything about cybersecurity—the ABA Third Edition Cyber-Security Handbook is 693 pages.

No matter how careful, it is impossible to make your client data completely secure. The ethics opinions recognize this. Attorneys' duties are to take reasonable precautions, which require attorneys to understand how client information is stored and transmitted, where vulnerabilities may be, and to know and reasonably use the tools and techniques of cybersecurity.

If you want further information on any of the tools or techniques, recommendations for particular programs, or summarized ABA Formal Ethics Opinions, contact the author at Joel@SelikLaw.com.

JOEL G. SELIK is a member of the Nevada Standing Committee on Ethics and Professional Responsibility. With offices in Nevada and California since 1985, he practices primarily judgment collection, and legal and medical malpractice.