Chicago Daily Law Bulletin®

Volume 163, No. 129 Serving Chicago's legal community for 162 years

High-tech security devices abound; make sure your clients are protected

With e-mail hacks and data thefts on the rise, sole practitioners must be extra vigilant in safeguarding client information.

Beyond financial and reputational risks, a breach of client confidentiality could violate the Rules of Professional Conduct, including Rule 1.1 (duty of competence requires knowledge of "benefits and risks associated with relevant technology"), Rule 1.4 (client's right to make "informed decisions regarding the representation") and Rule 1.6(e) (requiring "reasonable efforts" to protect "information relating to the representation of a client").

Informed security choices with client consent

The ethics rules do not prescribe specific methods to protect e-mails or data. Instead, lawyers are advised to make their own informed choices, with client consent, based on the sensitivity of the information, the likelihood of disclosure and the costs and difficulties of using safety measures.

Last May, the American Bar Association issued Formal Opinion 477, which proposes a sliding scale of protections, based on the need for confidentiality arising from the representation.

For "routine" client e-mails, the ABA says, unencrypted e-mail "generally remains an acceptable method of lawyer-client communication." However, e-mail encryption or other safety measures may be needed for "higher risk scenarios," such as matters involving "trade secrets, mergers and acquisitions or industries with "a higher risk of data theft."

Further, all client e-mails, encrypted or not, should be labeled as "privileged and confidential" and include a standard "confidential-e-mail-for-recipient-only" disclaimer.

To protect other client data, the ABA suggests several baseline measures, such as secure Wi-Fi; virtual private networks; firewalls; anti-virus, anti-malware and anti-spyware programs; and maintaining updated operating systems.

More sensitive information, the ABA goes on, may require additional protections such as data encryption, secure cloud-based storage systems, remote disabling of devices that are lost or stolen and even hand-delivery if warranted by the circumstances.

Lastly, lawyers are advised to discuss the risks with each client, reach a consensus on the best course of action and make sure all safety procedures are followed by the firm's employees and outside vendors.

If you haven't thought about cybersecurity in a while, here are some simple and inexpensive ways to help protect client information. (These suggestions do not supplant each lawyer's obligation to evaluate the risks and determine appropriate methods of protection based on his or her circumstances, following consultation with the client.)

Secure your phone and tablet

Smartphones and tablets can be invaluable tools for solo attorneys on the go, but they require some basic precautions in the event of theft or loss.

First, keep intruders at bay by requiring a password when the unit is turned on or when the screen times out. More modern devices allow fingerprint scanning and even facial recognition, to make the activation process safer and faster.

Next, install a program that allows you to locate a lost phone or tablet, lock the screen, leave a contact message for anyone who finds the device and even remotely wipe the contents if necessary. Between Google's Android Device Manager and Apple's Find my iPhone app, every practitioner should use this free safety feature.

Encrypt your desktop and laptop

While many solos enjoy the flexibility of using laptops, or have desktops in shared office spaces, these conveniences carry an increased risk of theft. Encryption can be used to deny computer thieves physical access to your hard drive.

SOLE SPEAK

GLENN E. HEILIZER

Glenn E. Heilizer is a veteran litigator and sole practitioner based in Chicago and is the founder of the Sole Practitioners Bar Association of Illinois. He handles commercial disputes in the federal, state and appellate courts in Illinois and Wisconsin. He welcomes all questions and comments, and he can be reached at glenn@heilizer.com.

Encryption protects the drive by requiring a password, tied to a lengthy recovery key, when the unit is powered up. Many computers now include a "trusted platform module," which is activated on encrypted devices and provides additional protection if the drive is removed and examined through a separate docking station.

Microsoft's Bitlocker encryption program is free with Windows 10 Pro and with certain earlier Windows versions. Mac computers use a similar program called FileVault, available on OS X Lion and later editions.

Encryption is relatively simple and well worth the effort. Back up your data first and save your password and recovery key in a safe place.

Encrypt e-mails when needed

Although Formal Opinion 477 accepts unencrypted e-mail for "routine" client communications, practitioners should discuss encryption with clients and be prepared for this option if warranted.

For users of Outlook or Gmail, Virtru offers a simple and free solution. Open an account at virtru.com, and receive an easy-to-use plug-in, which allows encryption of e-mail and attachments with a simple mouse click. Recipients can read, download attachments and reply through Virtru's secure reader portal.

For $5 per month, you can also revoke sent e-mails, make them expire when desired and prohibit forwarding to third parties.

Password confidential documents

When sending a confidential document for the client's eyes only, consider using a secure password that you provide the client by phone. Programs like Adobe Acrobat Pro and Microsoft Word include simple password features. Passwords later can be removed for more general use if desired.

Web-based attorney-client portals

If you prefer a more global security approach and are willing to spend roughly $500 or more per year, check out an all-in-one solution with an online service such as MyCase. Secure client communications and document exchanges are included among numerous other practice management features. With a free 30-day trial, followed by a monthly charge of $39 per user, MyCase is an attractive alternative for sole practitioners.

Address security issues in retainer letter

Make sure to discuss security risks and communication alternatives with the client and include a section in your retainer letter that reflects your understanding. Per the comments to Rule 1.6(e), clients may "require the lawyer to implement special security measures not required by this rule" or alternatively "forgo security measures that would otherwise be required by this rule."

Make sure you and the client agree on applicable security measures for your case and document your agreement.

In sum, sole practitioners must take steps protect client information from evolving threats. According to Formal Opinion 477, we live in a "world where law enforcement discusses hacking and data loss in terms of "when" — not "if." Address the risks now, and you may avoid significant problems down the road.