KAUFMAN | DOLOWICH

Cracking the Code: How To Navigate a Lawyer's Duty To Avoid Phishing Attacks, By Courtney Curtis-Ives & Robert Borowski, The Recorder, 12-13-2022

Until California courts adopt a legal standard, the best practice is to strive for "reasonable efforts" both before and after a potential visit from a cybercriminal.

By Courtney Curtis-Ivesand Robert Borowski

Attorneys in California are facing an increase in cyber liability claims asserted by their clients and sometimes by third parties arising out of email phishing attacks. The Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) defines phishing attacks as "email or malicious websites to solicit personal information by posing as a trustworthy organization." Let's suppose a former client sends an email out of the blue asking for the review of a document.

Or perhaps an email is received with wire instructions from opposing counsel regarding where to send settlement funds. It may appear harmless, but on the "other side" of a seemingly legitimate transaction could be a cybercriminal impersonator. One wrong click and they have control. Today's schemes have become so elaborate that nearly every lawyer is at risk. This is evidenced in part by the drastic rise in acquisition of cyber insurance policies.

So, what is the standard of care that will or should be imposed on an attorney if they, or their clients, are victimized by such an attack? Unfortunately, and despite the increase in cases, this issue has barely reached California courts if at all. Only as recently as March 2021 did the California Supreme Court add the duty of technology competence to the California Rules of Professional Conduct (CRPC). Found in Comment 1 to CRPC 1.1, this is today an important benchmark for attorneys which states that the duty of competence now includes "the duty to keep abreast of the changes in the law and its practice, including the benefits and risks associated with relevant technology."

The State Bar of California Standing Committee on Professional Responsibility and Conduct has advised that there are primarily two professional obligations triggered when dealing with technology—the duty of confidentiality and the duty of competence (Cal. State Bar Formal Opn. No. 2010-179). The committee has issued a few advisory opinions on a lawyer's obligations related to technology in recent years, but admittedly recognizes that "guidance to attorneys in this area has not kept pace with technology."

As a result, the committee's approach discussed in Cal. State Bar Formal Opn. No. 2010-179 has been one of flexibility: "Rather than engage in a technology-by-technology analysis, which would likely become obsolete shortly, this opinion sets forth the general analysis that an attorney should undertake when considering use of a particular form of technology." The Committee went on to identify six different factors for attorneys to consider before using a specific technology, which do not provide much guidance on potential liability for phishing attacks since email is now a universally accepted method of communication.

The Committee more recently refined its guidance in Cal. State Bar Formal Opn. No. 2020-203. Citing guidance from ABA Formal Opn. No. 18-483, attorneys must use "reasonable efforts" to protect against email phishing attacks. What exactly that means is open to interpretation. The ABA poses that "reasonable" depends on a number of factors including the sensitivity of the information. For highly sensitive information, the ABA advises the best practice may be to use encrypted software, discuss cybersecurity measures with a client beforehand, and/or obtain consent to transmit information through certain platforms.

For matters of normal or low sensitivity, the ABA believes "standard security methods with low to reasonable costs to implement" should be sufficient. Although notably, the committee and the ABA both reject "requirements for specific security measures (such as firewalls, passwords, or the like)." Rather, the committee advises that "reasonable efforts" should be determined by looking to the attorney's entire "process."

Accordingly, it seems the best way for attorneys to protect themselves is by addressing their obligations in two phases: 1) Before the Breach, and 2) After the Breach.

Before the Breach

ABA Formal Opn. No. 477R discusses a number of basic techniques attorneys can use to contribute to their "reasonable efforts." These include but are not limited to using secure Wi-Fi networks, using complex passwords and changing them regularly, multi-factor authentication and implementing antivirus software on all devices being used. CISA also issued a report, entitled Security Tip ST04-014, and cautions individuals to beware of suspicious email addresses, generic greetings and signatures, misspelled website URLs and strange/foreign domains, poor spelling and grammar, as well as suspicious or unexpected attachments.

CISA further advises the best thing to do when encountering any of these factors may be to independently try to verify the sender through phone or internet searches. Overall, attorneys must be mindful to "minimize particular identified risks."

After the Breach

It is impossible to guarantee complete protection from phishing attacks given the evolving sophistication of cybercriminals. As a result, an attorney's conduct after a breach has occurred is equally if not more important. The Committee advises attorneys must "act reasonably and promptly to stop the breach and mitigate damages resulting from the breach."

At minimum, this should include 1) cutting off the source of the breach, if possible, 2) informing the client about what has occurred and 3) taking steps to investigate what happened. Common investigative efforts can include working with internal IT departments, talking with outside security experts, reporting the incident(s) to the relevant authorities and flagging payments to any banks if funds have been wrongfully disbursed. The Committee also advises that law firms should consider having a uniform data breach response plan in place to facilitate coordination of mitigating efforts (more details can be found in ABA Formal Opn. No. 18-483).

Until California courts adopt a legal standard, the best practice is to strive for "reasonable efforts" both before and after a potential visit from a cybercriminal.

Courtney Curtis-Ives is a partner in Kaufman Dolowich & Voluck's Los Angeles office and co-chair of the firm's Professional Liability Practice Group. She focuses her practice on defending professionals in malpractice actions, with an emphasis on representing law firms. Ccurtis@kaufmandolowich.com.

Robert J. Borowski is an associate in the firm's Los Angeles office and focuses his practice on the defense of civil litigation matters with an emphasis on lawyer's professional liability. Rborowski@kaufmandolowich.com.