PETTITKOHN
PETTIT KOHN INGRASSIA LUTZ & DOLIN

Lawyers' Obligations Regarding Cyberattacks

As the holders of sensitive client information, lawyers present an attractive opportunity for hackers. These attacks can take the form of phishing emails, ransomware, and data breaches among other risks. High profile attacks on Adobe, Sony, Target, and Marriott emphasize the risks for lawyers and the need to address those risks. ABA Formal Opinion 483 quoted Robert Mueller noting that there are two types of business entities in the world – those that have been hacked and those that will be.

Preventing Attacks
Lawyers have a duty to keep certain types of information received from their clients confidential. This means they need to take proactive steps to prevent cyberattacks. This includes researching relevant technology, implementing that technology, and educating employees about risks. The ABA Standing Committee in Formal Opinion 483 noted the duty to provide competent representation includes understanding the benefits and risks associated with relevant technology.

The Opinion noted this includes using and understanding technologies in a manner that will reasonably safeguard property and information entrusted to the lawyer. This requirement can be satisfied by the lawyer doing his own study and investigation or by retaining qualified employees. Notably, the Opinion further noted that lawyers must also make reasonable efforts to monitor their technology in order to prevent, and detect, breaches. The Opinion noted that a security breach does not necessarily mean an ethical violation has occurred, but the subsequent failure to detect a breach and advise the client could result in a violation.

Responding to Attacks
When a data breach is either suspected or detected, RPC 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate any damage caused by the breach. Lawyers should consider developing an incident response plan with specific procedures in place for responding to a data breach.

A lawyer should also determine whether electronic files were accessed, and if so, which ones. This information gathering process is necessary for a lawyer to understand the extent of the intrusion and to enable the lawyer to make a full disclosure to the client, consistent with the lawyer's duties of communication and honesty under RPCs 1.4 and 8.4(c).

Rule 1.4 provides that a lawyer must keep the client reasonably informed and explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation. Thus, when a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information, a lawyer has a duty to notify the client of the breach.

Conclusion
Lawyers need to embrace technology in today's legal environment. This includes the ethical obligation to take proactive steps to protect information systems, to prevent cyberattacks and to respond appropriately when a cyberattack or data breach occurs.

Douglas A. Pettit

Douglas A. Pettit is a Shareholder with extensive trial and litigation experience, focusing on business litigation and professional liability. He is a member of the American Board of Trial Advocates, has a Martindale-Hubbell AV Rating, and was recognized as Best Lawyers' San Diego Legal Malpractice Lawyer of the Year 2015, 2018.