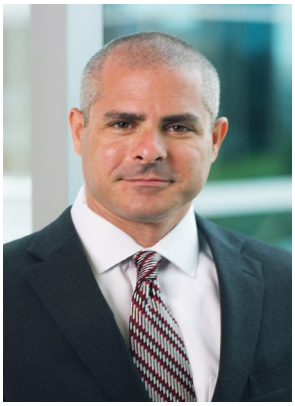
NEWMEYER & DILLION LLP

COMPANIES: PER THE AMERICAN BAR ASSOCIATION, HERE ARE YOUR ATTORNEYS' OBLIGATIONS RELATED TO CYBERATTACKS

By: Joshua B. Bevitz



Joshua Bevitz

Contact

925.988.3200
Joshua.Bevitz@ndlf.com

Practice Areas

Business Litigation
Construction Litigation
Cybersecurity
Insurance Law
Real Estate Litigation

As cyberattacks begin to become more and more frequent, the American Bar Association ("ABA") continues to issue opinions regarding the ethical duties of attorneys in relation to them. On October 17, 2018, the ABA issued yet another, Formal Opinion 483.

Formal Opinion 483 allows companies to better understand their attorneys' obligations to guard against cyberattacks, to protect the electronic information provided to them, and to respond if an attack occurs. An attorney's failure to adhere to these guidelines could result in damage to your business.

I. Attorneys have an ethical duty to protect their clients against cyberattacks.

Model Rule 1.1 states: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." Comment 8 to Rule 1.1 reads, "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." (Emphasis added.)

As it relates to cyberattacks, Formal Opinion 483 specifies, "Lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data and the use of data." That is, as with paper files, lawyers have the same obligation to ensure the security of electronic files.

However, a successful cyberattack does not necessarily mean an attorney has committed an ethical violation. Rather, an ethical violation only results if the attorney did not take reasonable steps to protect its electronic files.

II. Attorneys have ethical duties to address cyberattacks through proactive incident response plans, investigations, and proper notifications.

Incident Response Plan.

When a cyberattack is successful, Model Rule 1.1 requires an attorney to stop the attack and mitigate the damage. As such, the ABA recommends that attorneys have a preexisting incident response plan in place with specific plans and procedures for responding so that any damage and disruption resulting from the attack can be minimized.

The incident response plan should also outline who has been tasked with carrying out each step in addition to who is assigned the overall duty to ensure that the incident response plan is undertaken. Moreover, Formal Opinion 483 specifically states that "a competent lawyer must make all reasonable efforts to restore computer operations to be able again to service the needs of the lawyer's clients."

Investigation.

Formal Opinion 483 also specifies that a competent attorney must make reasonable attempts to make sure the attack has been stopped and to determine what happened, including whether data was lost or accessed. The investigation should yield sufficient information so that the attorney can make accurate disclosures to his clients that are consistent with the ethical duties of honesty and communication.

Notification to Current Clients – Depending on the Breach.

Formal Opinion 483 states that cyberattack notification requirements "will depend on the type of breach that occurs and the nature of the data compromised by the breach." Notification to the client is required if material client information has actually "been accessed, disclosed or lost in a breach" or if it reasonable to suspect as much. The notification should be sufficient for attorney's clients to make informed decisions regarding the next steps to take.

An attorney should also notify clients that reasonable steps were taken to determine exactly what information was affected and advise them of a plan to deal with it, such as potentially trying to recover lost information or taking steps to fortify cybersecurity. Formal Opinion 483 also concludes that an attorney must reasonably keep his clients apprised regarding post-attack developments.[1]

Law Firms - Per The ABA, Take The Following Actions To Protect Your Current and Former Clients and Yourselves.

Current Clients

Cyberattacks on law offices will only increase in frequency given the sensitive and potentially valuable information in electronic client files. Attorneys should take reasonable actions to do all of the following:

1. Protect your computer system and ensure your vendors are doing the same;
2. Have an incident response plan in place to stop the attack and minimize the damage;
3. Conduct an investigation to determine exactly what happened; and
4. Notify and advise clients as required.

Former Clients

Formal Opinion 483 treats former clients differently because the Model Rules do not address an attorney's duty to notify a former client of a cyberattack.[2] The Committee did note that, pursuant to Rule 1.16(d), attorneys should avoid retaining client files indefinitely.

---

[1] Importantly, an attorney has legal duties separate from ethical duties. As such, if personally identifiable information of a client is affected, an attorney should comply with any applicable privacy laws and other statutes, including as to their notification requirements.

[2] Again, even though an attorney may not have an ethical duty to notify a former client of cyberattack, an attorney should still comply with notification requirements pursuant to any applicable privacy laws and other statutes.

As such, Formal Opinion 483 recommends that attorneys reach agreements with clients at the end of representation regarding how electronic files will be handled. Absent agreements, the Committee recommends that attorneys follow an electronic document retention schedule to reduce the amount of client information they retain. Following those recommendations could reduce the chance of legal exposure if a successful cyberattack in fact occurs.

Failure to adhere to these guidelines could result in damage to your current and former clients. It could also lead to your own civil liability and land you in ethical hot water.

Joshua Bevitz is a partner in Newmeyer & Dillion's Walnut Creek office, and a member of the firm's Cybersecurity practice. As an experienced Insurance litigator, Josh advises his clients on proactive measures and potential pitfalls related to their cyber insurance policies. For questions on how you can protect your business, you can reach Joshua at Joshua.Bevitz@ndlf.com.

ABOUT NEWMEYER & DILLION LLP

For more than 30 years, Newmeyer & Dillion has delivered creative and outstanding legal solutions and trial results for a wide array of clients. With over 70 attorneys practicing in all aspects of business, employment, real estate, construction and insurance law, Newmeyer & Dillion delivers legal services tailored to meet each client's needs. Headquartered in Newport Beach, California, with offices in Walnut Creek, California and Las Vegas, Nevada, Newmeyer & Dillion attorneys are recognized by The Best Lawyers in America©, and Super Lawyers as top tier and some of the best lawyers in California, and have been given Martindale-Hubbell Peer Review's AV Preeminent® highest rating.

For additional information, call 949.854.7000 or visit www.ndlf.com.