Utah Bar® JOURNAL

Volume 32 No. 1
Jan/Feb 2019

Spring Convention registration inside.

I've Had a Data Breach. Now What?

by Keith A. Call

In 2017, a law firm cybersecurity consulting firm released an astonishing report about law firm cybersecurity. *See* LogicForce, *Law Firm Cybersecurity Scorecard, 2017 Q1*, https://www.logicforce.com/2018/03/28/law-firm-cyber-security-scorecard/. After conducting surveys and assessments of more than 200 law firms ranging in size from one attorney to more than 400, LogicForce reported:

- "Every law firm assessed was unwantedly targeted for confidential client data in 2016–2017."
- Approximately 40% of those law firms did not even know they were breached.
- Across the law firms surveyed and tested, there were on average 10,000 intrusion attempts per day, per server.
- 4.2 billion records were compromised across 4,169 publicly confirmed breaches in 2016.
- Cyberattacks on law firms are non-discriminatory. Size and revenues do not mater.

Several years ago, I had a run of about three consecutive years of free credit reporting. Apparently, my personal credit card information had been compromised after using it at some of the nation's largest and most sophisticated retail companies. I have not had any similar problems for the past few years (knock on wood!). I wonder if internet security protocols at major retailers have improved.

My personal suspicion is that hackers are turning their attention to easier targets – like law firms. Law firms often possess a host of incredibly valuable information as part of their electronic databases, including clients' intellectual property, tax returns, bank and other financial information, business plans, medical records, and other personal client information. Large and sophisticated businesses and financial institutions have made great strides to improve internet security, but law firms may not be keeping up. One industry consultant writes, "Law firms are notorious for having low levels of data security in place…even worse than the clients they are serving." *See* Erika Winston, *Why Hackers Target Law Firms* (May 25, 2017), https://www.timesolv.com/why-hackers-target-law-firms/.

Unfortunately, no matter how large or small your law firm is, it is no longer a question of whether you will be attacked, but when. *See* Jim Calloway, *Manage Cyber-Attacks: Is It Really Not If You Will be Attacked, But When?*, Law Practice Tips Blog (June 8, 2017), https://www.lawpracticetipsblog.com/2017/06/-manage-cyber-attacks-is-it-really-not-if-you-will-be-attacked-but-when.html.

In the September/October 2017 issue of the *Utah Bar Journal*, I addressed a lawyer's ethical obligations to secure client communications and other information in an electronic world. I discussed ABA Ethics Formal Opinion No. 477R, which explained a lawyer's ethical duty to use reasonable efforts when communicating client information over the Internet. *See* Keith A. Call, *Securing Communication of Protected Information in an Electronic World*, 30 Utah B. J. 38 (Sept./Oct. 2017).

Recently, the ABA issued Formal Opinion 483, which picks up where Opinion 477R left off: What are an attorney's ethical obligations after a data breach has exposed confidential client information? ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 483 (2018). The Opinion identifies several ethical *duties* a lawyer has after a data breach, as well as several not-so-binding *best practices*. Here are some highlights.

Monitor for Security Breaches.

Lawyers must employ reasonable efforts to monitor their technology and office resources connected to the Internet, external data sources, and external vendors. "[J]ust as lawyers must safeguard

KEITH A. CALL is a shareholder at Snow Christensen & Martineau. His practice includes professional liability defense, IP and technology litigation, and general commercial litigation.

and monitor the security of paper files and actual client property, lawyers utilizing technology have the same obligation to safeguard and monitor the security of electronically stored client property and information." *Id*. at 5. Without reasonable monitoring, a lawyer could be oblivious that client information has been compromised.

Stop the Breach and Restore Systems.

The Opinion suggests that lawyers and law firms develop an incident response plan *before* a lawyer is swept up in a breach. A good response plan identifies specific individuals who can and will identify and evaluate any potential intrusion, assess its nature and scope, determine if confidential information was actually accessed and compromised, quarantine the threat, prevent the exfiltration of information from the firm, eradicate the malware, and restore the integrity of the firm's network.

Determine What Occurred.

"Just as a lawyer would need to assess which paper files were stolen from the lawyer's office, so too lawyers must make reasonable attempts to determine whether electronic files were accessed, and if so, which ones." *Id*. at 7.

Preserve Client Confidences.

Unauthorized access to client information is not a violation of Model Rule 1.6 (preserving client confidences) if the lawyer has made reasonable efforts to prevent access or disclosure. *See* Model R. Prof'l Cond. 1.6, cmt. [18]. Opinion 483 cautions against compounding unauthorized access to client information in the process of responding to and reporting any data breach. For example, use extreme caution – and re-read Rule 1.6 – before disclosing confidential client information to law enforcement authorities without client consent.

Inform the Client.

Model Rule 1.4(a)(3) provides that a lawyer must "keep the client reasonably informed about the status of the matter." *See* Model R. Prof'l Conduct 1.4(a)(3). The ABA Ethics Committee concluded that whenever a data breach involves, or has a substantial likelihood of involving, material client confidential information, a lawyer has a duty to notify the client of the breach. Formal Op. 483 at 11. Disclosure is not required in ransomware situations if all client information was accessible to the lawyer at all material times. Similarly, disclosure is not required if no client information was accessed by the breach. Disclosure is required if material client information was actually or reasonably suspected to have been accessed, disclosed, or lost. The disclosure must be sufficient for the client to make an informed decision about what to do next and must include material developments in post-breach investigations. The Opinion stopped short of requiring disclosure to former clients but encouraged lawyers to reach agreements with clients about how the client's electronic information will be handled after the representation ends.

Consider Obligations under State and Federal Law.

The Opinion is limited to a lawyer's ethical obligations in the event of a data breach. But it points out that all fifty states have statutory breach notification laws. Federal laws and regulations may also apply. Lawyers should evaluate whether they must provide statutory or regulatory notification to clients or others, or take other action based on these cybersecurity laws.

In sum, it is helpful to think of your electronic files as paper files. You would likely take proactive steps if you knew someone had stolen or copied your client's confidential paper files. Similarly, you have to be proactive in the event of a breach of your electronically stored information. Opinion 483 provides some useful guidance to follow in the event your data systems are attacked and compromised.

Every case is different. This article should not be construed to state enforceable legal standards or to provide guidance for any particular case. The views expressed in this article are solely those of the author.