New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 263—NO. 41
TUESDAY, MARCH 3, 2020

State E-Discovery

Cybersecurity 'Hygiene' For Lawyers

By **Mark A. Berman**

Cybersecurity health is in-creasingly necessary for lawyers to keep their and their clients' information secure. The prevalence of "hacking," "ransomware" and "phishing" attacks, scams and other unauthorized digital intrusions demonstrates the need to use reasonable and appropriate technology to safeguard confidential and privileged information. Doing so is mandated by New York's Rules of Professional Conduct, as well as the recently enacted New York state "Stop Hacks and Improve Electronic Data Security" or "SHIELD Act," which applies to all law firms, even to solo practitioners and small firms.

SHUTTERSTOCK

MARK A. BERMAN *is a partner at Ganfer Shore Leeds & Zauderer and co-chair of the New York State Bar Association's Committee on Technology and the Legal Profession. He was the founding co-chair of the Social Media Committee of NYSBA's Commercial and Federal Litigation Section.*

Lawyer's Ethical Obligations

A lawyer must take reasonable care to affirmatively protect client confidential information and NYSBA Committee on Professional Ethics Op. 1019 provides that the duty of "reasonable care":

> does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered to determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.

NYSBA Committee on Professional

Ethics Op. 842 further provides that:

> [c]yber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cybercrooks. That is particularly true where there is outside access to the internal system by third parties, including law firm employees working at other firm offices, at home or when traveling, or clients who have been given access to the firm's document system … In light of these developments, it is even more important for a law firm to determine that the technology it will use to provide remote access (as well as the devices that firm lawyers will use to effect remote access), provides reasonable assurance that confidential client information will be protected.

Lawyers' Statutory Obligation

New York's SHIELD Act creates substantive security requirements for persons or businesses that hold the "private information" of New York residents, and it (1) expands the types of data that may trigger data breach notification to include user names or email addresses, and account, credit or debit card numbers; (2) broadens the definition of a breach to include unauthorized "access" (in addition to unauthorized "acquisition"); and (3) creates a new reasonable security requirement for companies to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of" private information. The SHIELD Act applies to all law firms and, as it applies to solo practitioners and small law firms, it requires those persons and entities to ensure that there "are reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers."

New York's SHIELD Act creates substantive security requirements for persons or businesses that hold the "private information" of New York residents.

'Key Takeaways' Report

To assist lawyers in complying with their ethical and legal obligations, the Committee on Technology and the Legal Profession of the New York State Bar Association, of which I am co-chair, recently issued a guide titled "Key Takeaways from the Cybersecurity Leadership Conference," identifying actionable and practicable steps lawyers may use to protect electronically stored information. "Key Takeaways" is concise and easy to read and contains critical information in addressing incident response, ransomware, risk management, and disclosures to clients and vendors and breach notification, as well as cybersecurity insurance. "Key Takeaways" seeks to educate attorneys, as further discussed below, so that they may be better able to have informed discussions with information technology professionals, cybersecurity vendors, insurance providers, and clients about cybersecurity issues, in order to improve their cybersecurity defenses and to ensure they are complying with their ethical obligations. The key is to make security a priority and to know what you have so that you know what and how to protect it.

Incident Response. Incident response requires a certain level of cybersecurity competence for both litigators and transactional attorneys in order to understand cyber risk management concepts. These include cyber threat literacy, pre-incident planning, incident response, and iteration, which means having an adaptive and dynamic approach to cyber incident responses. Lawyers need to understand the risks they face, such as financial fraud and compromised information, as well as to have an understanding of the technology lawyers' use that may facilitate attacks by "bad actors" on client and firm electronic information. Pre-incident planning takes a proactive approach to incident response. Educating staff is essential so that cyber risks are minimized and not passed on to clients. Firms should have guidelines for investigating and responding to cyber incidents. Response plans will assist on how to contain incidents, safeguard evidence of the attack, and identify and comply with applicable breach notification laws. Preparing these plans in advance will help assess

what changes may need to be made to stay secure.

"Ransomware" or "Phishing". A law firm employee may receive an electronic communication or "link" asking that he or she "click" on it as it purports to be relevant to something the person is working on or is related to the person's legal practice. A "bad actor" often studies targets in advance from what is publicly available online so he or she can craft urgent, time-sensitive and specifically tailored communications designed to convince the person to "click" on the link. Once the link is opened, the "bad actor" often can look at the firm's network for vulnerabilities, insert latent malignancies, or corrupt or make firm data inaccessible by encrypting it. The "bad actor" then may improperly use firm and client data, post it or sell it. An attorney may receive a voicemail or electronic communication indicating that the firm's data has been compromised and requiring a "ransom" payment to have it "returned" in an accessible form. It is important to train lawyers and staff on how not to be "suckered" to take such "bait." Law firm "social engineering" training is easily available.

Risk Management. IT professionals can periodically test a firm's network for vulnerabilities or put firm systems through "stress" tests or conduct "penetration" testing, and report back what "fixes" may need to be made to minimize the risk of compromise. It is important to convey to all law firm personnel that they are personally responsible for maintaining a high level of security consciousness. Keeping current with the newest versions of the technology platforms your firm uses and timely installing updates and "patches" is required as vendors seek to update their software to address vulnerabilities when they become apparent. Maintaining offsite backup of confidential data is critical. However, such backup needs to be configured so that it does not itself get compromised when an intrusion takes place. In addition, encrypt, as appropriate, firm and client data that is saved or transmitted.

Law Firm Disclosures. In the event of an attack, counsel must determine what international, state or federal laws, statutes and regulations may apply, and what obligations there are to also notify of the attack, pursuant to engagement letters and contracts with third-party vendors, or ethical obligations. Advising regulators and law enforcement needs to be addressed, and consideration given to discussing with them next steps. Do not forget that court orders need to be reviewed for compliance in the event of a compromise and advising opposing counsel may be necessary. Of course, counsel's insurance carrier needs to be notified immediately. Consideration must be given to the specificity of any breach disclosure, its timing and whether it should be appropriately delayed, and the manner of disclosure. Detailed guidance can be found in ABA Formal Opinion 483, *Lawyers' Obligations After an Electronic Data Breach or Cyberattack*, Oct. 17, 2018. In addition, while the nature of any disclosure needs to be based on the facts of the breach, the SHIELD Act provides, if notification is required, that a "description of the categories of information that were, or are reasonably believed to have been accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, accessed or acquired."

Cybersecurity Insurance. Cyber insurance should be second nature, like having legal malpractice insurance. It is relatively inexpensive. Such insurance, which should incorporate "social engineering" protection, would protect a firm from being "scammed" because a "con job" is not truly a "cyber" event and is more akin to fraud. Attorneys should always ask what is not covered by a firm's cybersecurity insurance, and ensure that it protects a firm against being "defrauded" not just out of monies belonging to the firm, but also out of client or opposing parties' monies held in escrow. Cyber insurance may cover a good portion of the costs and expense associated with loss transfer, breach coaches, a forensic review of the firm's network after an attack, legal expenses, and the expense of breach notification to clients.

GS L&Z Ganfer Shore Leeds & Zauderer LLP

360 Lexington Avenue
New York, New York 10017
212.922.9250
mberman@ganfershore.com