Attorneys on alert for cybersecurity threats: New York's new CLE training requirement

By John Bandler, Esq., Bandler Law Firm PLLC

JULY 19, 2023

July 1st was a cybersecurity milestone for every New York attorney who now needs to complete an hour of cybersecurity training before renewing their law license. New York Courts in their role supervising and licensing attorneys recognize the importance of cybersecurity, and the threat of cybercrime.

Cybercrime menaces every person and organization including attorneys, law firms and their clients. Attorneys have specialized duties that translate to cybersecurity obligations in addition to the general obligations that apply to other professions and sectors.

The cybercrime threats

Attorneys and law firms are lucrative cybercrime targets because they negotiate and settle deals and transactions of all types. Attorneys frequently send and receive instructions about where to wire funds — such as to transact real estate or settle a legal claim. Lawyers sometimes receive funds to hold in escrow, eventually to disburse to the proper destination (hopefully).

New York attorneys who renew their law licenses on or after July 1, 2023, will need to certify that they have completed one hour of cybersecurity training (continuing legal education, or CLE).

These are not perfunctory tasks though some are lulled into a false sense of security involving, for example, an inadequate routine. Cybercriminals steal billions of dollars each year by using email to trick victims into sending funds to the wrong destination.

Unwitting attorneys can play a role in furthering or preventing this fraud which may be called:

- Business email compromise;
- CEO Fraud;
- Email based funds transfer frauds.

While there are a variety of terms and scenarios for this crime, basically the cybercriminal impersonates one person using email and sends fraudulent bank wiring instructions to another. If successful, the funds are essentially sent to the cyber criminal instead of the rightful recipient. This fraud is not exclusive to attorneys but they are regularly involved in susceptible transactions. And nor is this the sole cybercrime danger that attorneys need to protect against; other priority threats include data breaches and ransomware.

The attorney duties and professional obligations for cybersecurity

Cybersecurity and cybercrime prevention are now solidly part of traditional attorney duties even though universal knowledge and compliance is not yet here.

Some attorneys might have chosen law to deal with words and not technology. But technology is a part of life and legal practice. Attorneys who do not understand technology or cybersecurity could be in danger of being negligent, comparable to an automobile driver who does not understand what traffic signs mean, what snow does to a road surface, or what the pedals on the car floor do.

The duty exists to drive knowledgeably and safely on the roads, and so does the duty to protect information systems and client confidences and funds. These attorney obligations in the age of cybercrime come from traditional duties of confidentiality, competence, communication, and the fiduciary duty to the client.

Life and legal practice extend to the cyber realm and as a result so do those longstanding duties. We can analogize various situations today involving technology with similar situations 40 years ago to see what is expected and acceptable and what falls below a necessary standard of care.

Attorneys also need to consider rules of general application since every state has a data breach reporting law, many states have cybersecurity requirements, and traditional laws of negligence and contract apply as well.

The ABA's early thoughts

The American Bar Association comments to the Model Rules of Professional Conduct provide further guidance and detail, and specifically emphasize that traditional duties of competence and confidentiality extend to technology and cybersecurity. Many of these comments on technology were put in place in 2012.

The ABA Standing Committee on Ethics and Professional Responsibility opinions have highlighted ethical and professional duties relating to cyber — an ethical duty to be competent with technology and cybersecurity to fulfil important duties and keep client information secure.

The committee's May 2017 Formal Opinion 477R on cybersecurity obligations for attorneys was a major update from its prior 1999 opinion (which addressed the relative novelty of email). At that time, I was making final corrections on my book "Cybersecurity for the Home and Office" (soon thereafter published by the ABA) so new Opinion 477 required a change which I was able to achieve with a footnote. In 2018 the ABA issued an ethics opinion on lawyer responsibilities after a cyberattack (Formal Opinion 483).

New York's attorney training requirement

New York attorneys who renew their law licenses on or after July 1, 2023, will need to certify that they have completed one hour of cybersecurity training (continuing legal education, or CLE). This new training requirement recognizes the importance of cybersecurity and having sufficient knowledge to make good decisions. The language of the new rule clearly connects existing ethical obligations and professional responsibilities to the protection of electronic data and confidential information.

Attorneys in New York register every two years, and part of that process is certification that they have completed 24 CLE credit hours. Some of those credit hours need to be devoted to specific topics and now cybersecurity is one of them. The cybersecurity training can be either in the area of cybersecurity ethics (which includes professional responsibility and complying with the duties of confidentiality and competence) or general cybersecurity, which encompasses more general knowledge about technology, cybercrime, cybersecurity and more.

The training is just one step among many for cybersecurity

This training requirement is not a box to be checked and forgotten, nor a CLE video to play in the background while half listening for the CLE code but mostly working on other matters. Instead, training is a tool to help attorneys learn and comply with other important professional responsibilities relating to cybersecurity and cybercrime prevention. Attorneys who neglect this area can face negative consequences.

Laws of general application also need to be considered, and New York attorneys should evaluate New York's SHIELD Act of 2019 which imposed a cybersecurity requirement for certain data and also strengthened the state's data breach reporting requirement. Many other states have cybersecurity laws and all states have data breach reporting requirements. Certain sectors (such as finance and health) have their specific rules as well.

A good practice for all attorneys?

Even if your state does not require cybersecurity training, improving your knowledge on cybersecurity and cybercrime is a good idea for all attorneys and other occupations too. You can meet your obligations, prevent a cybercrime, protect yourself, your organization, and your clients. When a cybercrime occurs, no one is happy and sometimes significant sums of money are stolen. Next events can include malpractice complaints, litigation, and damage to business and peace of mind.

Good cybersecurity and good management of information assets go together. This means we can both prevent bad events and improve efficiency and our management of technology. The carrot and the stick both motivate; cybersecurity and cybercrime provide both forms of persuasion.

Driver training is advisable before getting a driver's license because it can prevent accidents and help us better enjoy our driving experience with improved skills and decision making.

Now cybersecurity training is a requirement for New York lawyers. We can embrace this new rule as an opportunity to protect ourselves and our clients, and better use our technology.

John Bandler is a regular contributing columnist on cybercrime and cybersecurity for Reuters Legal News and Westlaw Today.

About the author

John Bandler is a lawyer, consultant, author, and adjunct professor at Elisabeth Haub School of Law at Pace University. He helps organizations protect from cybercrime, improve cybersecurity, and better manage information assets. He is the author of the 2017 book, "Cybersecurity for the Home and Office," published by the American Bar Association. His firm, based in New York, is **Bandler Law Firm PLLC**, and he can be reached at JohnBandler@JohnBandler.com.

This article was first published on Reuters Legal News and Westlaw Today on July 19, 2023.