George T. Holler is the founder of Milford-based Holler Law Firm LLC. The firm is one of the largest real estate practices in Connecticut.

Protect Your Clients and Your Practice

By George T. Holler

Interested in Learning more about this topic?

Attend ***Hacked: Counseling Clients after a Data Breach*** CLE on January 10.

Visit ctbar.org/calendar

The e-mail hit my inbox first thing in the morning. It was from a friend, and the tone was urgent:

"George—I have a client with a big problem. He was using a freelance paralegal to prep his closing. Her e-mail got hacked and the hackers sent the bank fraudulent wiring instructions. Now he has a conflict of interest and can't represent the buyer in fighting with the bank to get them to send a replacement wire. Buyer can't close and needs help. Can you assist?"

This came to me from a well-known legal ethics lawyer just last month. His client is the attorney who had been representing the buyer (and lender) in a purchase, and the story—an increasingly common occurrence—is every real estate practitioner's worst nightmare. I would argue the lawyer should not have been using a freelance paralegal in the first place, but in another recent case, an attorney in New York suffered a similar loss when her own AOL e-mail account was hacked.

Cyber-crime is a very real problem that is not going away anytime soon, and it is up to you to protect yourself. According to Joseph Gugliotta, inspector with the U.S. Postal Inspection Service, if you suffer a loss of under a million dollars due to cyber theft, the FBI will not even bother to investigate. You can submit your report online, but you are on your own when it comes to recovering those funds. Local police departments will help where they can, but much of the crime today is carried out by international operators, and as a result, the likelihood of prosecution is low.

So, what are the simple steps you can take right now to reduce your risk?

First, figure out where you currently stand. What are your weaknesses? Basic troubles arise from using free e-mail providers such as AOL, Hotmail, Yahoo, or Gmail.

Another common issue is something as simple as leaving files out in the open where people can access them—items left on your desk overnight, or in an area where someone from the outside can peer in through a window and see them, or worse, photograph them. Using contract employees or other outside service providers creates another set of potential problems.

Once you have completed this basic assessment, start by implementing simple solutions. You can create a hosted e-mail through sites like GoDaddy.com at very little cost. Install updated antivirus software on your network and make sure it is always kept current. Make your passwords more robust—at least nine characters with a number, symbol, and both upper and lowercase letters—and force users to change them at least once every 90 days. Your computers should also time out, i.e. they should go to sleep if not in use for a set period of time. It is easy to protect your physical documents by using lockable cabinets and drawers, and by utilizing a shredding service. When using outside service providers, be sure and have a non-disclosure agreement signed. While it may not guarantee they will not compromise your client's data, it will at least provide a level of protection against liability for you.

After you have implemented your most basic remediation, begin the process of documenting everything. Protecting data and minimizing your risk of cyberattack is a major undertaking, and you should treat it like you would any major project in your firm by having a written plan and following it. Matthew Froning, Chief Information Officer at Security Compliance Associates, a data security firm, explained to me that almost half of all security breaches are caused by employee or contractor negligence. It simply is not enough to put processes in place if people don't know what they are, and your team will not adhere to your policies if you fail to invest in training on those policies. None of this will be done adequately without a written protocol to follow.

I have spoken with many lawyers who constantly rail against the increased regulatory burden on small firms, particularly for real estate practitioners, but data breaches are a threat to all of us, as the recent Panama Papers imbroglio has taught us. We can pretend that it will not happen to us, or we can be proactive and take steps to protect ourselves. As my legal-ethics lawyer friend likes to say, "Better to avoid the problem than clean it up." **CL**