Cybersecurity Should Be Every Lawyer's Concern

Recent malware attacks put attorneys and law firms on alert

Witness some recent headlines:

- 66% of U.S. law firms reported a breach in 2016;
- Phishing emails are responsible for 91% of cyberattacks;
- Russian hackers are trading your credentials like magic cards;
- 40% of law firms underwent a security audit by a client and 18 firms lost a client for failing an IT audit;
- 95% of law firms were not compliant with their own data security policies.

Lawyers are soft targets for the hackers and criminals inhabiting the dark internet. We face substantial risks including the loss of client data, frozen computer systems and networks, substantial financial expenses, and notoriety and loss of reputation.

Eighty to 90 percent of all issues are due to human error. Phishing emails arrive daily and populate the inboxes of attorneys and staff already working at warp speed. The top reasons for errors include curiosity and urgency, and the consequences of an inadvertent click include malware, ransomware and financial intrusions. Defensive weapons must include password vigilance, employee training and education, constant vigilance, and, at this point in time, cybersecurity insurance.

The recent worldwide malware attack claimed numerous victims including the prominent global law firm, DLA Piper. More than most firms, DLA Piper was probably as well-armed as a law firm can be. Still, what may have been an inadvertent click by an employee in the Ukraine or Spain resulted in substantial interruptions of communications and operations, and might have inflicted significant financial losses.

We have no alternative except to consider seriously the purchase of cyber insurance. Malpractice insurers and general liability insurers are not willing to cover the losses that might result from malware or ransomware events. Attorneys may have been slow to recognize those facts, but perhaps as a result of the recent attacks, a noted cyber insurance company quadrupled its sales of policies in the most recent quarter compared to the first quarter of 2017.

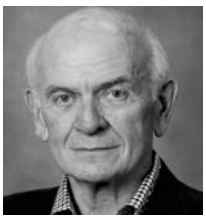
Our regular training and education for our personnel and in our offices must include constant attention to the power of passwords, penetration tests, and frequent reminders to attorneys and staff. NIST, a federal agency, has recently published password guidance for all federal employees that should be equally applicable to the protocols attorneys follow. Among its recommendations are longer passwords, using passphrases rather than complexly-structured passwords, and a comparison of the email addresses and passwords in use to known databases of emails and passwords known to have been exposed by massive hacks and cyber invasions such as the ones experienced by Sony, LinkedIn, and Dropbox. (Simple reminder: Test your email at https://haveibeenpwned.com/).

> **We owe it to our clients and to ourselves to increase substantially our use of encryption in our daily practices.**

You may have no experience with passphrases, but arguably they can be as robust as passwords of similar length. A passphrase is simply a sequence of words run together without the necessity of special characters and forced case changes. For instance, "mybrothersliveinClevelandandSyracuse", would take the hacker sitting on his bed about 300 trillion, trillion, trillion centuries to crack at the rate of a 1,000 guesses per second. That particular passphrase is not a true statement about my siblings' residence but is certainly easier to remember than "fnsleoW!*8P." "fnsleoW!*8P" is far more difficult to remember but much easier to break. The simple reason is that length is probably the best solution to achieving password security. (For an object lesson, test your passwords at Steve Gibson's Haystack: https://www.grc.com/haystack.htm.)

Finally, we owe it to our clients and to ourselves to increase substantially our use of encryption in our daily practices. All of our communications should be encrypted in transit as well as almost all their attachments. All of the data resting on the computers, systems and servers in our offices should be encrypted in place, and nothing should be stored in the cloud that is not well-protected by passwords, encryption and physical security.

Years ago, the cartoonist, Walt Kelly, created the long-running comic strip *Pogo*. His characters inhabited the Okefenokee Swamp and often commented on the human condition. Perhaps the strip's most famous quotation was: "We have met the enemy and he is us." Attorneys could well fit that description if they neglect their cybersecurity responsibilities.



Bill Kammer (wkammer@swsslaw.com) is a partner with Solomon Ward Seidenwurm & Smith, LLP.