Is it Possible to Secure Law Firm Data?

By Sharon D. Nelson, Esq. and John W. Simek

To answer the question, we interviewed our friend and colleague Matt Kesner, the CIO of Fenwick & West LLP, a West Coast law firm representing high tech and bio-tech clients. Matt has "walked the walk" when it comes to security and protecting data.

Is the data at a law firm really different or are there "special" considerations when dealing with security within a law firm? Matt suggested that there are a lot of tensions at play within a law firm. There's always the tension between IT and end-users. The end-users are more difficult to tame and are more independent than most other users. They don't necessarily want to comply with the stated policies and procedures, thereby making security a more difficult task. Also, they tend to be driven by what the client wants, which may be in contradiction to the security procedures of the firm.

The press hasn't really identified many data breaches that have involved law firms. Since law firms are very much reputation based, they are not all that willing to publicize any data breach that may have occurred. Current data breach laws have changed that practice, but we still don't hear of many specifics concerning law firms. Matt acknowledged that there have been two breaches at his own firm. His advice for security is to learn lessons from breaches so you can avoid a recurrence – at least a recurrence of the same sort of attack. Fortunately for Matt's firm, the security incidents did not involve access to their network. Both occurrences involved their website, which was hosted externally.

We are aware of some other firms being compromised, primarily through mobile devices and unprotected laptops. As a minimum you should have a lock code on your mobile device and the drives on laptops should be fully encrypted. Matt's excellent advice is "When in doubt, encrypt it."

Not to scare our readers (OK, maybe just a little), but Matt confirmed that law firms are seeing an increase in hacking attempts. Reviews of his own firm's logs show repeated "door rattles" and attempted infiltration of the network. They are being probed a lot more often, tested with various scripts being used to determine vulnerabilities and have experienced a higher proportion of successful malware and phishing attacks against their users.

Many attacks appear to be originating from China, which is consistent with our experiences gleaned from security investigations involving these attacks. Our own government has cautioned us that every cell phone and smart phone that goes into China has spyware downloaded on it by the Chinese communications infrastructure. This spyware pretty much has unfettered access to the data that you are sending and receiving even if it is encrypted in transit. Another concern is bringing laptops to China. Matt advised us to weigh the laptop before and after taking it to China as many times hardware monitoring devices will be installed in the laptop itself. He also suggested taking a disposable cell phone when traveling to China. Many in the security field have stated that we are seeing activity from China's "C-level" (rookie) hackers since law firm systems are fairly easy to penetrate. China isn't even wasting

the efforts of their “B-level” or “A-level” teams when attacking U.S. systems. Essentially, China’s entry level hackers are practicing on U.S. law firm networks before “graduating” to more advanced hacking activities. Matt told us that Chinese students actually take hacking classes and hack Western websites as part of their homework. Pretty scary stuff.

Increased usage of the Internet, voluminous amounts of data and the sharing of that data for legitimate purposes has made the task of security even more difficult. There are many more attack points as the data grows and reaches out to many more parties as part of our normal business activities. Matt cautioned us to be wary of USB flash drives that we obtain at conferences since they may be infected with malware such as the Stuxnet virus.

We queried Matt if there really is a fix for the security state that we are currently observing. The answer, as you might have guessed, is that there is no silver bullet for security. His primary advice is to partner with a trusted security advisor and be prepared to budget some funds for security. Your firm needs to be constantly vigilant since the security risks of tomorrow will be different from those we see today.

If you’d like to listen to our interview with Matt on Legal Talk Network’s Digital Detective podcast, you can find the podcast at http://legaltalknetwork.com/podcasts/digital-detectives/2011/07/is-it-possible-to-secure-law-firm-data.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com.