Clients Demand Law Firm Cyberaudits

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

Bank of America Merrill Lynch Audits Law Firm Cybersecurity

Three years ago, there was a collective gasp heard 'round the country the day the press reported that Bank of America Merrill Lynch was auditing the cybersecurity policies at its outside law firms, partly under pressure from government regulators.

Assistant General Counsel Richard Borden stated that Bank of America is "one of the largest targets in the world" for cyberattacks, and that law firms are "considered one of the biggest vectors that the hackers, or others, are going to go at to try to get to our information."

Regulators at the Office of the Comptroller of the Currency, which oversees BofA and other financial services companies, "have focused on law firms," according to Borden. "They are coming down on us about security at law firms. So we have no choice but to check the information security and to audit — to actually audit — the information security of our law firms that have confidential information. We spend a lot of money and use a lot of law firms, so this is casting a very wide net."

Amid much hand-wringing, the prophecy that law firms would be forced to confront their data security shortcomings has finally come true. Clients now want, as do regulators, assurance that law firm data is being adequately protected. The receipt of information security audits, more politely termed "assessments", is now a regular occurrence at many law firms. They come not only from clients, but from insurance companies offering cyber insurance – but they want to know what they are getting into first!

Pay Now or Pay Later

Though law firms are not thrilled about lifting their data security skirts for inspection, this move was inevitable. For way too long, most law firms have paid scant attention to information security. We are hoarse from explaining that it is a "pay now or pay later" proposition – either law firms get serious about guarding their client data and spend the monies to do so – or they will pay later when a data breach causes them to require the services of digital forensics experts to investigate the breach and an outside lawyer to advise them of their legal responsibilities. They will also incur the costs of remediating the vulnerabilities and the costs associated with complying with state data breach notification laws (currently, 47 states have such laws).

The big firms have gotten the word. Previously, some clients have wanted to see law firm security policies. Some have allowed law firms to effectively audit themselves. Today, clients want to see if security policies and plans are actually being followed. And they want independent third party audits, sometimes including penetration testing.

As clients have woken up to the potential vulnerabilities of law firms, they are demanding much, much more in the way of security – it is clear that clients are leaving firms which don't meet their security expectations. Hence the fairly sudden desire to get secure. In the AmLaw 200 in 2015, firms were reported to be spending an average of 1.9% of gross revenues on cybersecurity – and that can amount to as much as $7 million a year. That is an extraordinary change, to say the least.

A Small Question of Ethics

This whole topic is hot, hot, hot – and it shows on the lecture circuit. Colleague Dave Ries sent a hypothetical currently being used for discussion in a CLE. The bulk of it was developed by the General Counsel of Buchanan Ingersoll & Rooney. It goes like this:

Prior to being hired as counsel for GRU [Genetics-R-Us], DCH [Dewey, Cheatham & Howe] must meet certain GRU security requirements. GRU has stringent security requirements for its service providers, including law firms. Lawyer 1 and Lawyer 2 are meeting with DCH's Technology Director to discuss GRU's security requirements and a questionnaire about security that GRU has asked the law firm to complete. Tech Director says that the firm meets most of the requirements, but not all of them. It will take weeks, or perhaps months, to comply with all of them. Lawyer 2 tells him "we have to tell the truth, but put our best foot forward and stretch things a little if you have to. I'd hate to lose this work because you haven't done your job. Just fill it out so we pass and sent it back to GHR. It's all tech stuff, so Lawyer 1 and I don't need to review it."

So what happened to the duty to supervise? Is the lawyer implicitly sanctioning deceit? Can you be competent under the new rules of professionalism when you say "it's all tech stuff" as though you had no need to investigate and understand it? This has all the makings of an ethical disaster.

Today, when we lecture on encryption, we have standing room only audiences. The people who come to our live sessions radiate a hunger for cybersecurity knowledge. They are genuinely scared – and perhaps more so because of the new versions of the ABA Rules of Professional Conduct 1.1 (Competence) and 1.6 (Confidentiality of Information), which together require competent and reasonable measures to safeguard information relating to clients. As we go to press, Virginia has just become the 18th state to adopt the changes to those rules – and it is clear that more states will be following suit soon.

How Do You Survive a Cyberaudit?

1. Be prepared for everything (including telling the truth).
2. Review your ethical responsibilities (better now than when you are before a Disciplinary Board).
3. Make sure you have a diagram showing where all your data is.
4. Be especially careful about third parties holding your data – you may need to audit them! At the very least, you need to understand their security precautions and procedures.
5. Do an annual review of all policies and plans which impact data security and update them as needed. These may include but not be limited to:
    - Business continuity plan
    - Disaster recovery plan
    - Incident response plan
    - Remote access policy
    - Employee termination policy
    - Password policy
    - Encryption policy
    - Data access policy (including access by guests/vendors/clients)
    - Physical security plan
    - BYOD/BYON policy
6. At least once a year, get a full-blown security assessment by an independent third party security company (if you are a smaller firm, use a smaller security firm – the prices are much less). Remember that these firms are in the business of making assessments – their own credibility is on the line, so their assessments carry more weight. As a bonus, you may get a discount from your insurer on your premiums.
7. Consider whether you need penetration testing – actual attempts by experts to breach your network. Penetration testing can include network attacks and/or physically attempting to penetrate your facility to access the computing infrastructure. This may be overkill for a small firm, but certainly not for a large firm.
8. Be prepared – make sure you have cyberinsurance that will protect you fully in the event of a data breach – most policies will not and require a specific rider.
9. Stop kowtowing to the demands of lawyers that they want to BYOD (bring their own device) or BYON (bring your own network). This is serious stuff, not a parlor game where willful children should rule.
10. Our advice? And yes, we're serious – law firm business should only be conducted on devices issued by the law firm – and no personal business should be allowed on those devices. Not many firms will have the gumption to do this (see the willful children remark above) but this will be a key measure valued by clients and regulators.

11. Encryption is not complicated. Make sure lawyers use it where needed!
12. If a cloud provider has a master decrypt key, encrypt before depositing any sensitive data there (e.g. Dropbox).
13. Install hardware and software that does realtime intrusion detection – if you are a smaller firm that can't afford this, make sure you enable logging so there will be a trail to follow.
14. Twice a year, have mandatory security training to keep employees advised of new security threats and to underscore the need for vigilance, including being watchful for suspicious e-mails, texts, hyperlinks etc. as well as social engineering ploys.
15. Document all your security measures so you can produce it as part of an audit.
16. Even if you are allowed to self-audit, don't. The human tendency is to cut corners or say "I think so" which translates to "yes" in the audit when you are not really sure "yes" is the full or correct answer.
17. If you're big enough, have an audit committee with players from IT, Compliance, Management, and Security. They will all have a part to play and it is important to get buy-in across the board.

It is impossible in a short article to describe all of the steps a law firm should take when confronted by an audit – they will likely be spelled out for you by your clients. With a little help from Google, search for "security audits checklist" and you'll find plenty of reference material.

Final thoughts

The time to get started on all this is yesterday. And we predict with a fair amount of confidence that many law firms will sashay into the future as vulnerable as ever unless clients force them to take security seriously.

We have all but throttled audiences in our passion to get them to understand how real the problem of data security is but in the end, perhaps Matt Hooper said it best when he prophesied in the original *Jaws* movie.

"I'm familiar with the fact that you are going to ignore this particular problem until it swims up and bites you in the ass!"

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