‘Legal Tech Lists’: 7 Ways Law Firms Invite A Breach

by Sharon D. Nelson, Esq., John W. Simek, and Michael C. Maschke

Why Would Law Firms Invite a Data Breach?

We fall back on the words of Forrest Gump. “Stupid is as stupid does.” 2023 was a very bad year for law firms – not only were many law firms breached – and some from BigLaw, but the class action attorneys have apparently discovered there is money to be made from class action lawsuits against breached law firms.

It seemed like a good time to talk about foolish things that law firms and lawyers do that amount to an engraved “breach me” invitation to cybercriminals.

They Don’t Adopt Multifactor Authentication (MFA)

As all lawyers know, there is an inconvenience factor to adopting MFA. And an amazing number of lawyers resist the very minor inconvenience of having to authenticate themselves twice, first entering their password (something they know) and then authenticating again via something they have (i.e. an app on their phone) or using biometrics.

According to Microsoft, the adoption of MFA will prevent 99.9% of account takeovers. We have seen multiple law firms refuse MFA (groaning about its inconvenience) only to suffer account takeovers. They sure were anxious to adopt MFA after the breach. D’oh.

Cloud Computing and Backups – The Rules That are Often Broken

Most importantly, you must have more than one backup – and one of the backups should not be connected to your network. The first thing cybercriminals will do after breaching your network is to break into any accessible backups so you cannot recover from the breach without paying the ransom. Also, make sure your cloud backup has multiple versions and doesn’t only sync the contents of the local backup. Encrypting the local backup shouldn’t replicate so that your cloud backups are encrypted too.

It is also important to recognize that, while having your data in the cloud is not a guarantee that you won’t be breached, your data is infinitely safer in the cloud. While there have been cloud breaches, MOST of them have happened because an employee of yours misconfigured something in the cloud. We’re down to only two clients who have their data on-premise – one is stubborn – and we feel for the other because that law firm is commanded by a major client to have the data onsite.

The cloud is where it’s all happening these days. If you cling to the past, you do yourself no favors – and note that some IT folks will encourage staying with an on-premise solution because they make more money that way.

Who Needs Cybersecurity Awareness Training? Not Us Surely . . .

Law firm employees are your first line of defense. Endless phishing emails (which have gotten more sophisticated thanks to artificial intelligence) and social engineering are dire threats. So why wouldn't you train employees to recognize these kinds of attacks – and offer them as many different examples as possible of those attacks and others? And yet most law firms, particularly the solo/small/midsized firms, do not offer this training.

The cost of an annual cybersecurity training online session is modest – the cost of a data breach is immense. Tip: Get a reference from a fellow lawyer about cybersecurity firms who do good employee training at a reasonable fee.

Commonly Asked: What's an Incident Response Plan?

An incident response plan (IRP) may salvage your firm in the event of a breach and yet only 42% of firms have one. And we're pretty sure that many of the IRPs that do exist are either outdated or not quite up to snuff. Get some help from a cybersecurity professional who is accustomed to drafting these plans.

Minus a thorough plan, after a breach you will haplessly do all sorts of things that are wrong, done in the incorrect order, etc. And remember, there are penalties (lots of them) for not handling a breach correctly and reporting it timely. And did we mention the ethics rules?

Don't Trust Your Employees

Why? Because they take your data when they go to another firm. You see that in the headlines regularly. You also often see law firm bookkeepers embezzle money. Just do a search and you will see the necessity of having someone audit your books.

Hopefully, you do not allow sharing of passwords. But employees do it anyway. The usual excuse is that, for instance, a lawyer and a paralegal need to have access to one another's email. If one is compromised, both are compromised. Enforce your policy!

When you need a security assessment, do NOT let your IT folks do it. They have a vested interest in the outcome. We could go on, but you get the idea. To conflate Ronald Reagan's words, "if you **must** trust, then verify."

Don't Travel Abroad with Your Laptop Full of Law Firm Data

If you take your work laptop abroad, you take your chances. Some countries are more dangerous than others. We have seen a video of a laptop left in a hotel room in China and watched as two men entered the lawyer's room and downloaded the entire contents of the laptop.

Mind you, not every country is as dangerous as China when it comes to coveting a lawyer's data. But routinely, large firms have clean laptops which they loan out for trips abroad. For small firms, the cost of an extra laptop or two is well worth it. Make sure you make this a law firm policy requirement.

Remember the post roll call words of police Sargeant Phil Esterhaus on Hill Street Blues? "Let's be careful out there." Those words apply here – and there may be ethical implications as well.

Don't Let Apps Have Access to Your Contact Info

We routinely see lawyers do this. MANY apps ask for access to your 'Contacts' and the average lawyer simply allows it. What are they thinking???? Your 'Contacts' contain all kinds of sensitive data – and the integrity of most apps is highly questionable. Many sell data.

Several bars have already said it is unethical to allow apps to access your 'Contacts.' And they are right!

This list could go on and on, but following the advice above should upgrade your cybersecurity significantly!

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com*

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional. mmaschke@senseient.com*