What Will You Do When Your Law Firm Is Breached?

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

Note that we did NOT title this article, "What Will You Do If Your Law Firm is Breached?" The reason is simple – experiencing a data breach is not an "if" – it is a "when." Just ask the IRS and the Office of Personnel Management. Mind you, their approach to information security was sloppy. Lawyers cannot afford, ethically, to have slipshod security when protecting confidential data.

Incident Response Plans

We have often written about steps to secure your data but this time we are stressing that it is imperative that you are ready for a data breach. This means you need a plan, which tends to be called an Incident Response Plan (IRP), often focused on data breaches but "incidents" can refer to responding to ransomware, fighting attempted hacks or an insider accessing data without authorization.

Most large firms now have these plans in place, but many smaller firms do not. More and more, we are seeing clients and insurance companies asking to see your Incident Response Plan. In the face of ever-escalating data breaches, now is a good time to come up with a plan. After all, football teams don't get the playbook on game day!

The problem with all plans is that they don't survive first contact with the enemy. That's ok. Far worse is having no plan at all and reacting in panic with no structure to guide your actions. We see that all the time – the first hour you spend with a client after they know they've been breached is often called "the upchuck hour." It is not a happy time.

Don't go in search a template IRP. No two law firms are set up exactly the same and all have different business processes, network infrastructures and types of data. You need a plan customized to fit your firm – the smaller you are, the shorter the plan is likely to be. While a book could be written about IRPs, we are going to give you a condensed and, we hope, digestible overview.

The Elements of an IRP

- Name the position titles which will be responsible for the functions listed in the IRP. Don't use names since people come and go. You need a broad-based team if you are a firm of any size – management, IT, information security, human resources, compliance, marketing, etc. Have a conference call bridge line identified in case a breach happens at night or on the weekends and include home/cell phone numbers and personal as well as work e-mail addresses. This list will need to be updated regularly as people join or leave the firm.
- Identify the contact information for a good data breach lawyer – many large firms now have whole departments working with data breaches. Don't think you can handle this without an attorney who specializes in data breaches. Your data breach lawyer (if you selected a good one) will be an invaluable quarterback for your IRP team – and he or she may be able to preserve under attorney/client privilege much of the information related to the breach.
- Identify the location of your insurance policy (which darn well better cover data breaches). You need to make sure you are covered before you start and list the insurer's contact information because you are going to need to call your insurer as soon as you are aware of a possible breach.
- Identify the contact information for law enforcement – perhaps your local FBI office – often the first folks called in.
- Identify the contact information for the digital forensics company you would want to investigate and remediate the cause of the breach. Generally, you will have been breached for six months or more before you discover the breach – it will take time to unravel what went on. You'll want to know if all data that should have been encrypted was indeed encrypted in transmission and in storage. If it was, this may lessen your notification burden. Identify any PII (Personally Identifiable Information) that may have been compromised.
- If you have intrusion detection or data loss prevention software, those logs should be provided to your investigators immediately and preserved. If you don't, you may want to think about implementing such software.

- Identify the contact information for your bank in case your banking credentials have been compromised.
- (Optional but often useful) Identify the contact information for a good public relations firm. If you are not required to make the breach public, you may not need one, but if it does go public, you may need to do some quick damage control. Your insurance coverage may provide for this, in which case the insurance company will put you in contact with the appropriate firm.
- How will you handle any contact with clients and third parties, remembering that you may wish not to "reveal all" and yet need to achieve some level of transparency? Be forewarned that this is a difficult balance. You will feel like the victim of a data breach, but your clients will feel as though you have breached their trust in you. A data breach that becomes public can cause a mass exodus of clients so work through your notification planning with great care. Be wary of speaking too fast before facts are fully vetted – this is a common mistake, trying to limit the damage and actually increasing it as the scope of the breach turns out to be far greater than first known.
- How will you handle informing employees about the incident? How will you ensure that the law firm speaks with one voice and that employees do not spread information about the breach in person or online? How will your social media cover the breach, if at all?
- If you have a data breach notification law in your state (and almost all do), put it right in the plan along with compliance guidelines. You may be required to contact your state Attorney General. These laws vary widely so be familiar with your own state law.
- If you have HIPAA, HITECH or other regulated data that may be impacted, make sure the relevant data breach regulations are referenced in the plan and attached to it.
- Does the breach require that IT and information security policies be changed? Does what you learned from the breach require that the IRP itself be revised? The IRP should mandate an annual review even without an incident.

Dress rehearsals

Yes, you do want to rehearse for a data breach. Add and subtract factors. Add a terrorist threat, subtract key personnel who are on a cruise, yada, yada. This is most often done as a tabletop exercise, one that should take place at least annually.

You will find that your needs and responses to a breach may evolve over time. For instance, as ransomware saw a 4000% increase in 2014, it became apparent that many back-up systems needed to be re-engineered so that they wouldn't be impacted by Cryptolocker, CryptoWall and their many variants. The threats will no doubt morph over time – as will the defenses.

Employee training

Make no mistake about it. The most successful attack against law firms is spear phishing - a targeted attack where the attacker has done some reconnaissance. They may know what cases you're involved in, who the opposing counsel is, the nickname of a senior partner, etc. This makes it easy to send what looks like a "genuine" e-mail, which in reality contains a malicious hyperlink or an attachment.

Training employees to be skeptical and to refrain from being click happy and to think about the e-mail they see in their Inbox is invaluable. We've seen firms which have successfully avoided a breach simply because an employee had enough sense to question whether a very well-done phishing e-mail was real.

If you question the monies spent on training or the loss of billable time, stack those costs up against the financial damage of a data breach and you'll see the absolute need for annual training. According to Verizon's 2015 Data Breach Investigations Report, almost 30% of data security incidents were due to human error. Persuaded yet?

Vendor Management

This could be the subject of an entire article, but just take our word for it. The security of third party vendors that have "hooks" into your network is critical for you to understand. Just ask Target which got compromised because an HVAC contractor was breached and the contractor had administrator access to Target's network. Make sure you understand a vendor's information security and don't

permit vendors to have access to any data they don't need. A vendor management policy is now a key law firm policy – we only started seeing these in the last year or two. If you don't have one, this too should be high on your priority list.

Final words

We recently read a white paper which was entitled, "Breach Preparation: Plan for the Inevitability of Compromise." It occurred to us that lawyers are very resistant to that idea, sometimes worried about cost or maybe just burying their heads in the sand and hoping that no bad guys zero in on them. While a data breach is indeed a nightmare, you are far more likely to survive it if you have a plan. This is not the time to be sanguine that you can survive hacking attempts when so many mighty entities have fallen victim.

Complacency and inaction are not your friends. Lawyers love risk management. The surest pathway to data breach risk management is to be prepared.

The authors are the President and Vice President at Sensei Enterprises, Inc., a digital forensics, information security and legal technology firm based in Fairfax, VA. 703-359-0700 (phone) 703-359-8434 (fax) sensei@senseient.com, http://www.senseient.com.