Incident Response Plans Come of Age

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

WHY DO ONLY 25% OF LAW FIRMS HAVE INCIDENT RESPONSE PLANS?

One of the most striking findings of the ABA's *2018 Legal Technology Survey Report* was that only 25% of law firms had an Incident Response Plan (IRP). In a world struggling daily against cyber incidents and data breaches, that is a piteous statistic. We don't know why so many law firm fail to create incident response plans, but it is time to come to grips with the necessity of having an Incident Response Plan. The last time we focused on this subject in an article was in 2015. It is definitely time to revisit the topic and issue a rallying cry for the adoption of IRPs.

Let us be clear at the outset that we are zeroing in on solo, small and mid-sized law firms. While large law firms will include all the elements we reference below in their IRPs, theirs will be far more complex and with many moving parts. As ever, we are trying to craft a solution that is reasonable and not financially overwhelming to meet the ethical rules which govern lawyers.

WHAT DOES AN IRP PREPARE YOU FOR?

An incident response plan prepares you for data breaches and cyber incidents. And we'll stop right there because we know many folks are confused by the difference. There are lot of cyber incidents that are not breaches. A common example is ransomware, where your data is encrypted, but not (in almost all cases) compromised. The whole point is to get you to pay a ransom, not to access and take your data.

Another common cyber incident involves someone pretending to be a law firm managing partner (spoofing their email) and asking the recipient to buy iTune cards. This happened to a local law firm on a new employee's first week of work. Because the email promised reimbursement and appeared genuine, she bought the cards. She was out $1200.00. No, the law firm did not make good her losses. Hopefully, her job at the law firm improved from there.

A true data breach is where your confidential data is actually accessed – and often transported (or exfiltrated, as the cybersecurity experts call it) to servers

elsewhere. This is the ultimate nightmare, triggering all manner of legal and ethical requirements.

An IRP can also prepare you for disasters, natural and manmade. Earthquakes, fire, floods, terrorist attacks, extended power outages, total system meltdowns, damage done by disgruntled employees, epidemics, biological attacks – the list goes on and on. In many law firms, there is a separate Disaster Recovery Plan or sometimes it is called a Business Continuity Plan to cover disasters. For our purposes, we are going focus on an IRP as dealing **solely** with cyber incidents and data breaches.

A STATISTIC, A QUOTE AND AN ANECDOTE

The 2018 ABA report referenced above showed that 23% of law firms have been breached at some point. In all likelihood, the percentage is much higher because many lawyers, especially in big firms, haven't the slightest clue that their firm has been breached unless the incident becomes public. The truth is that most law firm breaches never become public.

Some years ago, the authors attended a meeting in DC involving a number of AMLAW 200 law firms. While we were asked to keep all identifying details private, we can say that every law firm represented at that meeting had been breached, some more than once. It takes a lot to shock us, but we were shocked that day.

As for the quote, it is an oldie but a goodie – and by a man everyone knows today.

"I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again." Those words were spoken by former FBI Director Robert Mueller at the RSA Cybersecurity Conference in March 2012.

From our foxhole, that prediction has come true.

WHAT DOES ETHICS HAVE TO DO WITH INCIDENT RESPONSE PLANS?

When you have a cyber incident, a number of ethical requirements may come into play. On October 17, 2018, the ABA released Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack." That opinion built on the ABA's Formal Opinion 477R released in May 2017, which set forth a lawyer's

ethical obligation to secure protected client information when communicating digitally.

The new opinion states: "When a breach of protected client information is either suspected or detected, Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate damage resulting from the breach."

The opinion discusses Model Rule 1.1 (competence), Model Rule 1.4 (communications), Model Rule 1.6 (confidentiality of information), Model Rule 1.15 (safekeeping property), Model Rule 5.1 (responsibilities of a partner or supervisory lawyer) and Model Rule 5.3 (responsibilities regarding nonlawyer assistance).

There is a "rule of reason" to the opinion, which states, "As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach. . . The decision whether to adopt a plan, the content of any plan and actions taken to train and prepare for implementation of the plan should be made before a lawyer is swept up in an actual breach."

Cybersecurity experts have said the same thing for a very long time – and, in our experience, all large firms tend to have an incident response plan. The smaller firms are much less likely to have one. No one is saying that a law firm need to be invincible because that is not possible. As the opinion states, “the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach.” Everywhere we go to lecture, we stress “reasonable efforts” – and that has a whole lot to do with the size of the law firm as well as the sensitivity of the data it holds.

Both opinions should be read carefully – and probably more than once.

THE NUTS AND BOLTS OF IRPS

There are certain things common to all IRPs and we will discuss them. But let us begin with a caution: Don’t just grab a template from the internet and call yourself done. Templates can be useful starting points, but not more than that. Every law firm is unique in its structures, procedures, etc. Its IRP should reflect that.

Cybersecurity consultants can help with developing an appropriate IRP and so can data breach lawyers. It makes us chuckle to think that, not many years ago, no one called themselves data breach lawyers. Now data breach lawyers are spawning like rabbits. A short visit to Google will produce one near you.

WHO'S IN CHARGE?

One of the first things to identify in the IRP is the person who will manage a cyber crisis. You want a steely-eyed, calm individual who will keep a floundering ship steady in rough seas. Our experience is that such individuals exist, but are in short supply.

The person in change is going to receive a lot of bad advice. That means they must be true leaders, able to sift the good advice from the bad and yet make everyone feel included in the process. No easy task.

If you're a solo lawyer, your selection process is easy. You do it all and have no choice. But for everyone else, this is a choice of critical importance. Moreover, you need a backup in case the selected individual is unavailable for whatever reason.

YOUR FIRST FIVE CALLS

Before disaster strikes, hopefully you have already established a relationship with a data breach lawyer and a digital forensics firm (often the lawyer will recommend a firm). Here, as ever, there is a difference between large firms and smaller firms. The large firms tend to select a large firm data breach lawyer with a hefty price tag. Smaller firm are better served by a data breach lawyer from a smaller firm with a smaller price tag.

That same reasoning applies to the selection of a digital forensics firm. In selecting both a data breach lawyer and a digital forensics firm, the best advice we can offer is to consult your colleagues for recommendations if you don't already have these folks on board. However, if you have cyberinsurance coverage, the insurance company may designate law firms or companies.

There are arguments about whether to call the data breach lawyer or the digital forensics firm first. That's actually a close call in our judgment. You want to get preliminary advice from your lawyer as soon as possible, but you also want the

digital forensics folks to jump on board quickly because they may be able to take rapid measures to stop or limit the impact of the cyber incident.

Make sure these first two steps are in your IRP with contact info for the professionals you will be using.

Your data breach lawyer will advise you about whether it is necessary to call your regional FBI office or the FBI's Internet Crime Complaint Center (known as IC3) and located at https://www.ic3.gov/default.aspx. The IC3 has been particularly effective in cases involving wire fraud.

The next part of your plan will include calling your bank (if appropriate) to alert it in case there is any possibility that your funds are at risk – for instance, if the credentials to log into your operating or escrow account may have been compromised. Don't let this unnerve you – banks are used to getting these calls today. They are happy to flag your account so that they are especially alert to suspicious activity. That's a win-win.

Finally, you want to include contact information for your insurance company. Hopefully, you have by now secured cyber insurance (if not, put that on your priority list!). Most policies require notice within a certain amount of time and you may lose benefits if your notice is not timely.

NETWORK DIAGRAMS, LOGGING ETC.

Your IRP needs to reference a number of things about your infrastructure. Attached to the plan should be a network diagram, a detailed inventory of your hardware, and all relevant logging information – critical to an investigation of a cyber incident. You should always log as much as possible to create an audit trail of what may have happened – greatly appreciated by your digital forensics investigators.

This part of the IRP always creates a lot of headaches because this information tends to grow stale. At a smaller firm, it may be fine to update this annually, but a larger firm may need to revisit this information more often.

DATA BREACH NOTIFICATION LAWS

All the states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands now have data breach notification laws. Lucky you if you only practice in a

single jurisdiction. Just make sure you've read the law and place a copy of it with your IRP.

For those of you who practice in multiple jurisdictions, across the country, or internationally, you have a much bigger headache. This is where a data breach lawyer is invaluable. Beyond telling if you need to comply with state data breach notification laws (and what each law requires you to do), a data breach lawyer can assist with international compliance.

In all likelihood, the majority of folks reading this are practicing law only within the U.S. But beware, the laws vary widely – and carry penalties. Good legal advice is worth its weight in gold. Why don't we have a national data breach law? A very good question to which we have no good answer. A national data breach law has been proposed many times only to die in Congress. We imagine it will come one day because it is terribly confusing and expensive to comply with the national patchwork of laws.

COMMUNICATING DATA BREACHES WITH CLIENTS

Since data breaches cannot entirely be avoided, Formal Opinion 483 says of lawyers, "When they do (have a breach), they have a duty to notify clients of the data breach under Model Rule 1.4 in sufficient detail to keep clients 'reasonably informed' and with an explanation 'to the extent necessary to permit the client to make informed decisions regarding the representation.'"

So yes, this goes on the list of things to do if you have a breach, rather than a cyber incident.

First, law firms must halt the attack, mitigate the damage and then make reasonable efforts to assess the data that may have been exposed and the duty of disclosure. This is not so easy. There is ransomware which exfiltrates your data before encrypting your files (therefore a data breach) or ransomware which only encrypts your files and then asks a ransom for the decryption key (therefore not a data breach – and the much more common kind of ransomware). The opinion notes that your efforts in determining what happened and fixing it may be through qualified experts.

If you need to report an incident to a government agency, you are still bound by Rule 1.6. There is some tension over trying to report and trying to maintain client

confidential data. How do you know if the disclosure is "impliedly authorized?" Read the opinion fully to understand all the nuances of this dilemma.

What exactly are you supposed to tell clients in your disclosure? The opinion is a little vague, saying that "the disclosure must be sufficient to provide enough information for the client to make an informed decision as to what to do next, if anything."

The opinion dodges a bit when it comes to former clients, finding no duty to notify former clients unless there is something mandating notification. The IRP cannot possibly cover every scenario so it must simply provide for an analysis of whether and what to communicate to clients – and possibly third parties which may also be impacted by your cyber incident or data breach.

TESTING THE PLAN

You don't want a cyber incident to be your first test of your IRP. Annual tabletop exercises simulating a cyberattack are common and very useful. Adding and subtracting complications to a scenario is also helpful. What if your data breach lawyer is unavailable? What if the power grid is down? If the attack is on your cloud provider rather than on-premise servers, how does that change the plan itself?

Beyond tabletop exercises, security assessments are always a wise precaution – and yes, annual ones are optimum even for smaller firms. Penetration tests are where a good guy – hopefully a Certified Ethical Hacker, certified penetration tester such as GPEN or someone with a similar certification- simulates being a bad guy and attacks your firm to discover vulnerabilities. As we tell folks, this is not for the faint of heart and it tends to be considerably more expensive than a security assessment. Under the "reasonableness" standards of the ethics rules, we believe that the security assessment will suffice for most small to mid-sized firms.

FINAL WORDS

There is nothing magical about IRPs. They are "Plan A" and we all know that Plan A never survives first contact with the enemy. But at least you have a roadmap when a cyber incident strikes. We have seen hapless panic and foolish steps taken in the wake of a cyber attack many times – not a pretty sight and not useful under dire circumstances.

Inevitably, the plan will morph over time. There will be new threats, new defenses, new methodologies for investigating and recovering for a breach, etc. That's why these plans need regular review. But if you are part of the 75% of law firms without an IRP, it's time to roll up your sleeves and create one.

Sharon D. Nelson, Esq. 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 a co-author of 17 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 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.