# Your Law Firm Has Been Breached: Who Are You Going to Call?

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


**We've Had a Data Breach!**

No lawyer wants to hear those words about their law firm. But across the country, those words have been repeated time and again. How often? The ABA's *2021 Legal Technology Survey Report* tells us that 25% of respondents said that their law firms had a breach "at some time." That's a big percentage. Most law firms are ill-prepared for responding to a data breach with only 36% reporting that they have an Incident Response Plan (IRP). Understandably, 80% of law firms with 100+ attorneys do have an IRP.

If you have no IRP, you are asking for a catastrophe – and one likely to make the headlines. Roll up your sleeves and get to work creating one. Then do regular tabletop exercises on the IRP, adding and subtracting issues (electric grid compromised, managing partner inaccessible on a safari, etc.). Make sure the IRP is accessible during a disaster – we saw one data breach where the IRP was only in electronic form and it got encrypted with all the other data by a ransomware attack. "Whoopsie-Daisy" doesn't quite cover the extent of that debacle.

**Who Are You Going to Call?**

If you have an IRP, you have a plan which includes (in order) the steps you are going to take and the names of those you are going to call, with contact information. If you don't have an IRP, you are likely to panic – some victims are literally paralyzed by shock. Since we get a lot of those calls, we became very interested in who should be called and when – and take note that even experts disagree on who to call first.

**Our #1 Pick is a Data Breach Lawyer**

We didn't pull that out of thin air. We've talked to all kinds of cybersecurity experts and a majority think calling a data breach lawyer is your logical first step. You should have someone in mind (and identified in your IRP), but if you don't, get referrals from colleagues.

Why the data breach lawyer? Frist, they know pretty much everything you need to know and they have a lot of experience dealing with data breaches. Data breach lawyers tell us it is helpful to the client to have a "coach" early on and one who knows how to handle the myriad laws, regulations and ethical duties associated with data breaches. They will help you devise a game plan, depending on the circumstances.

**Three Things to Do Quickly**

- Notify your cyberinsurance company – you can file a claim later, but put them on notice and plan to have a meeting to discuss what's covered under what circumstances, exclusions, etc. Does the policy cover the payment of a ransom? Some companies are backing away from ransom payments. Insurance companies may have recommended digital forensics companies or, if you have a preferred company you know of, the insurer may want to approve that company before they are engaged.

- Get a digital forensics firm onsite as soon as possible. These are the folks who figure out what happened, remediate the problems, figure out whether your data can be restored and determine whether your data was accessed or exfiltrated. Help them out before the breach by making sure you are using logging mechanisms. Logs help the digital forensics folks figure out what happened and how, pivotal to understanding how to move forward. While on the subject of logs, make sure you maximize the amount of data in the log files (both in type of data collected and time of retention) as the default settings are rarely adequate. Also, the logs should be stored in a protected and safe area. Cybercriminals will seek out and destroy or encrypt your logs in order to remove any evidence of their activities.

- Contact your regional FBI office – you can do that at https://www.fbi.gov/contact-us/field-offices. The agents who come out will ask a lot of questions and sometimes answer some of your questions or tender advice, but they will not remediate the problems – that's not their job. Recently, businesses who have suffered a breach tell us that it can take several days for the FBI to come out. We are starting to hear data breach lawyers recommend that you file a complaint with the Internet Crime Complaint Center (IC3) which is a part of the FBI. Their response time is much shorter. IC3's website is at https://www.ic3.gov/.

- Immediately review your state's data breach notification law with your data breach lawyer (yes all the states and U.S. territories have such a law). If you're a firm which does work nationally, you may have a lot to do. Don't forget to review the requirements of the states which have data privacy laws (currently California, Virginia, and Colorado) as well.

**Who Else Do You Need to Call?**

- It's a good idea to call your bank – many banks will put an alert on your account so that any substantial transactions are verified with the customer before they are processed.

- It's no fun, but if you truly had a data breach and not a cybersecurity incident, ethical rules require that you share information about the breach with your affected clients so they can be prepared for the possible impact of the release of the data that has been accessed or exfiltrated.

- Do you need help with public relations? If knowledge of the breach has hit the press or your clients, this may be critical help if you can afford it. Ransomware gangs, in particular, often release data to pressure you into paying the ransom.

**Last words**

Data breaches are no fun. So have a playbook in hand – your IRP. Review the plan at least yearly because threats and defenses are constantly changing. Train your employees on cybersecurity – not from a high-tech standpoint, but from a user's perspective. 82% of users will not recognize a well-crafted phishing email. There is no technology which can provide a silver bullet solution, so your best defense is both technology and training.

Prepare, practice, and revise your Incident Response Plan regularly. As writer/financial advisor Howard Ruff once wryly noted, "It wasn't raining when Noah built the ark."

***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*.*