What to Do When Your Data Is Breached

By Sharon D. Nelson, David G. Ries, and John W. Simek

January 2018

"When, not if." This mantra among cybersecurity experts recognizes the ever-increasing incidence of data breaches. In an address at a major information security conference in 2012, then-director of the Federal Bureau of Investigation (FBI) Robert Mueller put it this way: "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."

Mueller's observation is true for attorneys and law firms as well as small businesses through Fortune 500 companies. There have now been numerous reports of law firm data breaches. The FBI has reported that it is seeing hundreds of law firms being increasingly targeted by hackers. Law firm breaches have ranged from simple (like those resulting from a lost or stolen laptop or mobile device) to highly sophisticated (like the deep penetration of a law firm network, with access to everything, for a year or more).

Lawyers and law firms are beginning to recognize this new reality, but all too often they expose themselves to unnecessary risk simply because they don't have a response plan for security incidents and data breaches. Attorneys have ethical and common law duties to employ competent and reasonable measures to safeguard information relating to clients. Many attorneys also have contractual and regulatory requirements for security. Attorneys also have ethical and common law duties to notify clients if client data has been breached.

Compliance with these duties includes implementing and maintaining comprehensive information security programs, including incident response plans, for law practices of all sizes, from solos to the largest firms. The security programs and response plans should be appropriately scaled to the size of the firm and the sensitivity of the information.

Adapted from S. Nelson, D. Ries and J. Simek, "What to Do When Your Data is Breached,) *GPSolo*, Vol. 33, No. 1 (January/February 2016).

THE OLD MANTRA: KEEP THE BARBARIANS AT BAY

In a more innocent time, we really thought we could keep the barbarians outside the walls that guard our data. The analogy was protecting the network like a fortress, with strong perimeter defenses, sometimes compared to walls and moats. Alas, those days are gone.

For years, the emphasis was on keeping villains—cybercriminals, state-sponsored agents, business espionage spies, and hackers—out. We went from fairly simple antivirus software and firewalls to more sophisticated antivirus software and next-generation firewalls, and, finally, to enterprise anti-malware security suites, next-generation security appliances, data loss protection and other strong technical defenses. The widespread use of mobile devices and remote connectivity, making data available outside protected networks, has added new challenges for defense.

The defensive tools have gotten more sophisticated and more effective. Sadly, what we have learned is that all the would-be intruders were not only matching the good guys step for step, they were outpacing them.

It took a surprisingly long time for everyone to "get it"—but in the end, the security community realized that if the bad guys are smart enough and target a particular entity, they are likely to be able to successfully scale the walls we built to keep them out. And with that realization, "detect and respond" became the new watchwords in cybersecurity.

Mind you, we are still trying to keep the bad guys out—that is our first line of defense. But now that we know that our first line of defense is too often a Maginot Line for sophisticated attackers, we have moved forward in our thinking.

Although detection and incident response have been necessary parts of comprehensive information security for years, they previously had taken a back seat to protection. Their increasing importance is now being recognized. Gartner, a leading technology consulting firm, has predicted that by 2020, 60 percent of enterprises' information security budgets will be allocated for rapid detection-and-response approaches, up from less than 10 percent in 2014.

THE NEW MANTRA: IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER The increasing recognition of the importance of detection and response has been evolving for a number of years. It is a core part of the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0,* that was released in February 2014 (www.nist.gov/document-3766).

Although the framework is aimed at security of critical infrastructure, it is based on generally accepted security principles that can apply to all kinds of businesses and enterprises, including law firms. It provides a structure that organizations, regulators, and customers can use to create, guide, assess, or improve comprehensive cybersecurity programs. The framework, "created through public-private collaboration, provides a common language to address and manage cyber risk in a cost-effective way based on business needs, without placing additional regulatory requirements on businesses."

The framework allows organizations—regardless of size, degree of cyber risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure (as well as other information systems). It is called "Version 1.0" because it is supposed to be a "living" document that will be updated to reflect new technology and new threats—and to incorporate "lessons learned." (NIST released drafts of Version 1.1 for public comment in January and December of 2017 and plans to release Version 1.1 in early 2018.)

The core of the framework, its magic words, are "identify, protect, detect, respond, and recover," which should shape any law firm's cybersecurity program.

"Identify and protect" was where we started in the early days of cybersecurity—and while those words are still important, "detect and respond" have surged forward as a new focus—along with, of course, recovering from security breaches, no easy task. It is especially tough if you don't know you've been breached—and the average victim has been breached for seven months or more before the breach is discovered!

INCIDENT RESPONSE PLANS

The core of the respond function is advance planning. This means attorneys and law firms need a plan, usually called an incident response plan (IRP), which often is focused on data breaches, but "incidents" can refer to ransomware, attempted hacks, an insider accessing data without authorization, or a lost or stolen laptop or mobile device.

Most large firms now have these plans in place, but many smaller firms do not. More and more, clients and insurance companies are asking to review law firms' IRPs. In the face of ever-escalating data breaches, now is a good time to develop and implement a plan or to update an existing one. After all, football teams don't get the playbook on game day.

The problem with all plans is that they may not survive first contact with the enemy. That's okay. Far worse is having no plan at all and reacting in panic with no structure to guide your actions. The first hour that a security consultant or law enforcement officer spends with a business or law firm after the discovery of a data breach is very unpleasant. Kevin Mandia, the founder of Mandiant (www.fireeye.com) a leading security firm, has called it "the upchuck hour." It is not a happy time.

Don't rely on a template IRP. No two law firms are identical, and all have different business processes, network infrastructures, and types of data. Although templates may serve as a starting point, an IRP must be customized to fit the firm—the smaller the firm, the shorter the plan is likely to be. For a solo practice, it may just be a series of checklists, with who to call for what. Books and standards have been written about IRPs. (See "Further Resources" below for a few of our favorites.)

Qualified professionals also can be consulted for more details. The following is a condensed and, we hope, digestible overview.

THE ELEMENTS OF AN IRP

- **Internal personnel.** Identify the internal personnel responsible for each of the functions listed in the IRP. Identify them by position titles rather than by name because people come and go. A broad-based team is required for 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 a weekend, and include home/cell phone numbers and personal as well as work email addresses. This list will need to be updated regularly as people join or leave the firm.
- **Data breach lawyer.** Identify the contact information for an experienced data breach lawyer—many large firms now have departments that focus on security and data breach response, and some smaller firms have a focus on the area. Don't convince yourself that you can handle this without an attorney who is experienced 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 investigation.
- **Insurance policy.** 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.
- **Law enforcement.** Identify the contact information for law enforcement (perhaps your local FBI office), often the first folks called in.
- **Digital forensics consultant.** Identify the contact information for the digital forensics consultant you would want to investigate and remediate the cause of the breach. Often, a firm has been breached for seven months or more before the breach is discovered—it will take time to unravel what went on.
- **Containment and recovery.** Include in the IRP containment and recovery from a breach. A law firm that has been breached has an increased risk of a subsequent (or continuing) breach—either because the breach has not been fully contained or because the attacker has discovered vulnerabilities that it can exploit in the future.
- **Compromised data.** Determine the data that has been compromised or potentially compromised. 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 the notification burden. Identify any personally identifiable information (PII) that may have been compromised.
- **Systems logs.** Identify and preserve systems logs for your information systems. If logging functions are not turned on or logs are not retained, start maintaining them before a breach.
- **Intrusion and data loss logs.** If you have intrusion detection or data loss prevention software, logs from them should be preserved and provided to your investigators immediately. If you don't, you may want to think about implementing such software.
- **Your bank.** Identify the contact information for your bank in case your banking credentials have been compromised.

- **Public relations consultant** (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.

- **Clients and third parties.** How will you handle any contact with clients and third parties, remembering that you may wish not to "reveal all" (if notice is not required) 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 soon before facts are fully vetted—it is a common mistake to try limiting the damage only to end up increasing it as the scope of the breach turns out to be far greater or different than first known.

- **Employees.** 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?

- **Data breach notification law.** 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. Also, determine whether other states' breach notice laws may apply owing to residences of employees or clients, location of remote offices, etc. Make sure that the relevant data breach regulations are referenced in the plan and attached to it.

- **Other legal obligations.** Identify any impacted data that is covered by other legal obligations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or client contractual requirements, and comply with notice requirements.

- **Training on the plan.** Conduct training on the plan. Make sure that everyone understands the plan and their role under it.

- **Testing the plan.** Testing can range from a quick walk-through of hypothetical incidents to a full tabletop exercise. Include contacts with external resources to make sure that everything is up-to-date. This will help to make everyone familiar with the plan and to identify areas that should be revised**.**

- **Review of policies.** Does the breach require that IT and information security controls and policies be updated or changed? Does what you learned from the breach require that the IRP itself be revised? The IRP should mandate at least an annual review even without an incident.

FINAL WORDS: PREPARE NOW!

The new paradigm in security is that businesses (including law firms) should prepare for *when* they will suffer a data breach, not for *if* they may suffer a breach. This requires security programs that include detection, response, and recovery, along with identification and protection of data and information assets. Successful response requires an effective incident response plan. Attorneys who

are prepared for a breach are more likely to survive and limit damage. Those who are unprepared are likely to spend more money, lose more time, and suffer more client and public relations problems. ■

Additional Resources

ABA Standing Committee on Law and National Security, *A Playbook for Cyber Events,* Second Edition (American Bar Association 2014)

Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, *Computer Security: Incident Handling Guide,* National Institute of Standards and Technology Special Publication 800-61, Rev. 2 (August 2012)

Federal Trade Commission, *Data Breach Response: A Guide for Business* (September 2016)

ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management (a consensus international standard)

Jason T. Luttgens, Matthew Pepe, and Kevin Mandia, *Incident Response & Computer Forensics,* Third Edition, McGraw-Hill (2014)

National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (February 2014) (NIST released drafts of Version 1.1 for public comment in January and December of 2017 and plans to release Version 1.1 in early 2018.)

U.S. Department of Health and Human Services, Office for Civil Rights, *A Quick-Response Checklist* (June 2017)

U.S. Department of Justice Cybersecurity Unit, *Best Practices for Victim Response and Reporting of Cyber Incidents (*April 2015)

Sharon D. Nelson (snelson@senseient.com) is an attorney and president of Sensei Enterprises, Inc., a legal technology, information security, and digital forensics firm in Fairfax, Virginia. David G. Ries (dries@clarkhill.com) is Of Counsel in the Pittsburgh, Pennsylvania, office of Clark Hill, PLC. John W. Simek (jsimek@senseient.com) is vice president of Sensei Enterprises, Inc. Nelson, Ries, and Simek are co-authors of *Encryption Made Simple for Lawyers* (ABA, 2015) and *Locked Down: Practical Information Security for Lawyers, Second Edition* (ABA, 2016).