What to Do *When* Your Data is Breached

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

"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 FBI director 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."[1]

Mueller's observation is true for attorneys and law firms as well as small businesses and Fortune 500 companies. There have 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).[2]

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.[3]

Credit: N. Hanacek/NIST

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

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 antimalware 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.

Defensive tools have gotten more sophisticated and more effective. Sadly, what we have learned is that would-be intruders were not only matching the good guys step for step, but they were outpacing them. It took a surprisingly long time for everyone to comprehend, but in the end, we in the

There have 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 Practice Solutions is a regular feature brought to you by the Practice Management Resource Center (PMRC) of the State Bar of Michigan, featuring articles on practice management for lawyers and their staff. For more resources offered by the PMRC, visit our website at http://www.michbar.org/pmrc/content or call our Helpline at (800) 341-9715 to speak with JoAnn Hathaway or Diane Ebersole, Practice Management Advisors.

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.

security community realized that if the bad guys are smart enough to target a particular entity and are persistent 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. For example, 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.[4]

The new mantra: identify, protect, detect, respond, and recover

Recognition of the importance of detection and response has been increasing for a number of years. It's a core part of the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.[5] Although the framework is aimed at security of critical infrastructure, it's 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."[6]

The framework allows organizations—regardless of size, degree of 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). The framework's core is built on the magic words *identify*, *protect*, *detect*, *respond*, and *recover*, which should shape any law firm's cybersecurity program. The framework is called Version 1.0 because it is a "living" document that is updated to reflect new technology and new threats, and incorporate lessons learned.[7] For example, NIST released Version 1.1 of the framework in April 2018, which continues the same approach.[8]

We started with *identify and protect* 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, which is no easy task. It's especially tough if you don't know you've been breached—the median time from breach to discovery in 2017 was 101 days![9]

Incident response plans

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

It has been our experience that most large firms 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.[10] In the face of ever-escalating data breaches, now is a good time to develop and implement a plan or 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 leading security firm Mandiant (now a part of FireEye), has called it "the upchuck hour."[11] It's 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 be a series of checklists detailing whom to call for what. Books and standards have been written about IRPs. See "Additional Resources" in the sidebar on the following page 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 function listed in the IRP. Categorize personnel by position titles rather than 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/

Additional Resources

American Bar Association, *A Playbook for Cyber Events: Second Edition* (2014)

Cichonski, et al, *Computer Security: Incident Handling Guide, Recommendations of the National Institute of Standards and Technology, Revision 2*, Special Publication 800-61 (NIST, August 2012) <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>

Federal Trade Commission, *Data Breach Response: A Guide for Business* (September 2016) <https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf>

International Organization for Standardization, ISO/IEC 27035, *Part 1: Principles of incident management* and *Part 2: Guidelines to plan and prepare for incident response* (2016) <https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-1:ed-1:v1:en>

Luttgens, Pepe & Mandia, *Incident Response & Computer Forensics: Third Edition* (McGraw-Hill Education, 2014)

The Sedona Conference Working Group on Data Security and Privacy Liability (WG11), *The Sedona Conference Incident Response Guide, Public Comment Version* (March 2018)

US Department of Health and Human Services, Office for Civil Rights, *A Quick-Response Checklist* (June 2017) <https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf>

US Department of Justice, Cybersecurity Unit, *Best Practices for Victim Response and Reporting of Cyber Incidents* (April 2015) <https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf>

cell phone numbers and personal and work email addresses. This list will need to be updated regularly as people join or leave the firm.

Data breach lawyer

Identify an experienced data breach lawyer—many large firms now have departments focusing on security and data breach response, and some smaller firms have a focus on the area. Don't convince yourself you can handle the situation without an attorney 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

Locate your insurance policy, which better cover data breaches. Make sure you are covered before you start, and list the insurer's contact information because you'll need to call your insurer as soon as you're aware of a possible breach.

Law enforcement

Obtain contact information for law enforcement (perhaps your local FBI office), often the first folks called in.

Digital forensics consultant

Identify the digital forensics consultant you would want to investigate and remediate the cause of the breach. As was mentioned, firms have been breached for months or more before the breach was discovered; it will take time to unravel what happened.

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 it can exploit in the future.

Compromised data

Determine what data has been compromised or potentially compromised. Verify whether all data that should have been encrypted was indeed encrypted in transmission and storage. If it was, this may lessen the notification burden. Identify any personally identifiable information that may have been compromised.

Systems logs

Identify and preserve logs for your information systems. If logging functions are not turned on or logs are not retained, start maintaining them now, before a breach.

Intrusion and data loss logs

If you have intrusion detection or data loss prevention software, those logs should be preserved and provided to investigators immediately. If you don't, you may want to think about implementing such software.

Your bank

Obtain the contact information for your bank in case your banking credentials have been compromised.

Crisis communications consultant (optional but often useful)

Identify a good crisis communications firm. If you're not required to make the breach public, you may not need one; if the breach does go public, you may need to do some quick damage control. Your insurance coverage may provide for this, in which case the insurer will put you in contact with the appropriate firm.

Clients and third parties

How will you handle contact with clients and third parties, recognizing that you may not wish to reveal all (if notice is not required) but achieve some level of transparency? This is a difficult balance. You'll 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 notification

planning with great care. Be wary of speaking before facts are fully vetted; a common mistake is trying to limit 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 inform employees about the incident? How will you ensure that the law firm speaks with one voice and that employees don't spread information about the breach in person or online? How will your social media cover the breach, if at all?

> Attorneys who are prepared for a breach are more likely to survive and limit damage.

Data breach notification law

Since all states now have data breach notification laws, include your state's notification law 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 state's requirements. Also, determine whether other states' breach notice laws may apply based on residences of employees or clients, location of remote offices, etc. Make sure relevant data breach regulations are referenced in and attached to the plan.

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 or client contractual requirements, and comply with notice requirements.

Training and testing the plan

Conduct training on the plan. Make sure that everyone understands the plan and their role in it. Testing can range from a quick walk-through of hypothetical incidents to a full tabletop exercise. Include contacts with external resources to make sure everything is updated. This will help familiarize everyone with the plan and identify areas needing revision.

Review of policies

Does the breach require updates or changes to IT and information security controls and policies? Does what you learned from the breach require a revised IRP? 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—not if—they will suffer a data 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. ■

This article was adapted from Nelson, Ries & Simek, "What to Do When Your Data is Breached," GPSolo, Vol. 33, No. 1 (January/February 2016).

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 coauthors of Encryption Made Simple for Lawyers *(ABA, 2015) and* Locked Down: Practical Information Security for Lawyers, Second Edition *(ABA, 2016).*

ENDNOTES

1. Robert S. Mueller, III, Director, FBI, Remarks at RSA Cybersecurity Conference (March 1, 2012) <https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies>. All websites cited in this article were accessed July 17, 2018.
2. E.g., Sloan, *Firms slow to awaken to cybersecurity threat,* The National Law Journal (March 8, 2010) <https://www.law.com/nationallawjournal/almID/1202445679728/Firms-slow-to-awaken-to-cybersecurity-threat-/?slreturn=20180617015346>; Jackson-Higgins, *Law Firms under Siege,* DARK Reading (April 6, 2011) <http://www.darkreading.com/attacks-breaches/law-firms-under-siege/d/d-id/1135516>; Martínez-Cabrera, *Law firms are lucrative targets of cyberscams,* SFGate (March 20, 2010) <https://www.sfgate.com/business/article/Law-firms-are-lucrative-targets-of-cyberscams-3269938.php>; and Riley & Pearson, *China-Based Hackers Target Law Firms to Get Secret Deal Data,* Bloomberg News (January 31, 2012) <https://www.bloomberg.com/news/articles/2012-01-31/china-based-hackers-target-law-firms>.
3. ABA Standing Comm on Ethics and Professional Responsibility, *Formal Opinion 477: Securing Communication of Protected Client Information* (May 11, 2017) <https://www.americanbar.org/content/dam/aba/administrative/law_national_security/ABA%20Formal%20Opinion%20477.authcheckdam.pdf> and ABA Model Rules of Professional Conduct 1.1, 1.4, and 1.6.
4. Chuvakin, *New Research on Dealing with Advanced Threats,* Gartner Blog Network (February 24, 2014) <https://blogs.gartner.com/anton-chuvakin/2014/02/24/new-research-on-dealing-with-advanced-threats>.
5. NIST, *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0* (February 12, 2014), pp 4–5 and 7–9 <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>. NIST's mission is to "promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life."
6. NIST, *NIST Releases Cybersecurity Framework Version 1.0* (updated January 8, 2018) <www.nist.gov/news-events/news/2014/02/nist-releases-cybersecurity-framework-version-10>.
7. *Id.*
8. NIST, *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1* (April 16, 2018) <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.
9. Mandiant, *M-Trends 2018* (April 2018) pp 7–9 <https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf>.
10. Ries, *TECHREPORT 2017—Security,* ABA (2017) <https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security.html>.
11. Perlroth, *Finding the Cleanup Crew After a Messy Hack Attack,* New York Times (December 29, 2011) <https://www.nytimes.com/2011/12/30/technology/hacker-attacks-like-stratfors-require-fast-response.html>.