The New Mantra in Cybersecurity: Detect and Respond

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

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. Alas, those days are gone.

For years, the emphasis was on preventing villains – cybercriminals, state-sponsored agents, business espionage spies and hackers – out. We went from fairly simple anti-virus software to sophisticated anti-virus software and, finally, to enterprise anti-malware software security suites.

The products got better and better and better. Sadly, what we 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, we realized that if the bad guys are smart enough and target a particular entity, they are going 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 a Maginot Line for sophisticated attackers, we have moved forward in our thinking.

The NIST Cybersecurity Framework

In February of 2014, we had begun moving forward toward securing our data and the physical infrastructure protecting it when the National Institute of Standards and Technology released Cybersecurity Framework Version 1.0.

The framework provides a structure that organizations, regulators and customers can use to create, guide, assess or improve comprehensive cybersecurity programs. This came as a result of Executive Order 12636, issued in February of 2013, which called for "the development of a voluntary, risk-based Cybersecurity

Framework—a set of existing standards, guidelines and practices to help organizations manage cyber risks. The resulting 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.

The document is called "Version 1.0" because, much like our Constitution, it is supposed to be a "living" document which will be updated to reflect new technology and new threats - and to incorporate "lessons learned."

Here is where you find the magic words of the document, "identify, protect, detect, respond and recover" that 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!

What Does "Detect and Respond" Mean for Law Firms?

It means rethinking how you approach security of your data. Now that you know that you can't keep a determined intruder out, you know you need to detect them once they've penetrated your network. So you need technology and software that will help you detect that you've had what is called, in polite circles, "a cybersecurity event" – translate that to "a breach."

As you can imagine, you want to know of these "events" as soon as possible so you can take action. Today, there are technology solutions that identify "anomalies" in your network (things that are outside the norm) or that look for executables that are unknown but are behaving like malware or some other form

of cyberattack. While such solution may be beyond the need or the budget of solos and very small firms, you don't have to be very large to start considering heading down this road – the risks of not doing so are simply too great.

Some of these solutions include data loss prevention (DLP) software and appliances, electronic content management systems (ECMs) and Security Event Management systems (SEMS). When you meet with someone who can explain the various solutions to you, brew a pot of expresso – you're going to need to be highly focused to understand how one solution differs from another – this is really cutting edge technology that changes from month to month (if not day to day).

As for your response to your incident, that may vary. After the initial panic, you will want your in-house or outside technology consultants (and you are likely to need digital forensics technologists, who are more familiar with data breach investigations) to take a look at the situation and see what they can determine. They can also, once they understand what has happened, figure out how to "plug the hole" and otherwise mitigate the breach. Remediation of whatever caused the breach is key.

Hopefully, you already have an incident response policy and plan in place, no matter how big or small you are. For all but the smallest firms, there should also be an incident response team in place to implement the plan. At a minimum, you should have already identified who will be involved along with their appropriate role.

In all probability, you will want to call a lawyer familiar with data breach laws who can advise you on complying with any of the 46 state data breach notification laws. And if there is data protected by federal law (such as HIPAA data), you'll need advice on that front too.

Finally, one of the first pieces of advice you are likely to be given is to call the FBI. While that is anathema to most law firms, it is the appropriate course of action. Remember that the FBI makes no public statements about these investigations and doesn't show up in flak jackets or otherwise make a public display of your "cybersecurity event."

The ABA Cybersecurity Resolution

The ABA has weighed in on cybersecurity concerns, always a sign that the states may follow. On August 12, 2014, the ABA House of Delegates passed, without opposition, a new cybersecurity resolution, Resolution 109, which reads as follows:

RESOLVED, *That the American Bar Association encourages private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected.*

You might be forgiven for thinking as you read the resolution, "Wow, that really says a whole bunch of nothing." And you'd be right – it is really a cautionary resolution intended to raise awareness.

There is a back story to the resolution, which was, in its original format much longer. The original resolution appeared to command all law firms, large and small, to come up with a cybersecurity program that met national and international standards.

This met with fierce opposition from a number of ABA entities, including our own Law Practice Division. The resolution was submitted by the ABA Cybersecurity Legal Task Force and the Section of Science & Technology Law.

In answer to the controversy, the language of the Resolution (which stands on its own and is not governed by the accompanying Report) was watered down to the tepid version above. At the behest of other entities, language in the Report was also changed to make it clear that the Resolution was not attempting to make a change in lawyers' ethical duties and to add language recognizing that smaller firms could not be expected to adopt a program that made no sense considering their size and budget constraints.

Clearly, for small firms, the international and national standards cited in the Report appeared fearsome. There are standards for smaller firms.

The report states: “Small organizations, including small law firms and solo practitioners, can prioritize key cybersecurity activities and tailor them to address the specific needs that have been identified.” For help with this, you might check out NIST Interagency Report 7621: *Small Business Information Security: The Fundamentals*.” Written in 2009, it’s a bit dated, but many fundamentals remain the same.

Remember that the Resolution governs – not the Report. So if you hear a vendor quoting from the Report to get you to buy something, don’t think the Report operates to set standards you must meet.

One Last Shot Across the Bow

While it is true that “Detect and Respond” has set off a hue and cry, never forget that it is best for your law firm if you really can keep the barbarians outside the gates. We were reminded of this as we were writing this column– a news article appeared on our newsfeeds telling us that another law firm had suffered a data breach after a firm backup disk (apparently unencrypted) had been stolen from an employee’s locked car trunk. The best defense we currently have to protect law firm data is encryption. “Detect and Respond” is a mantra you need to adopt but don’t make the mistake of failing to adequately protect your data. Encryption is a law firm’s best friend when it comes to risk management. If you haven’t deployed encryption everywhere, now is the time. As a point of interest, Google is marching full steam ahead with its encrypt everything program. That’s a good cue that you should be doing the same thing.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone)
www.senseient.com