Your Law Firm Has Been Breached! Now What?

By Sharon D. Nelson, Esq. & John W. Simek

© 2012 Sensei Enterprises, Inc.

We hate to be the bearer of bad news, though we so often are, but law firms are increasingly becoming the targets of data thieves. Why bother trying to attack the sophisticated security systems of the government contractor providing a new military attack weapon? It is so much easier to compromise the LAW FIRM for the government contractor since they probably don't have very robust security measures. Essentially, the law firms are considered the "soft underbelly" when trying to breach the client's data.

Your Law Firm Has Been 'Pwned'

The newly admitted attorneys should recognize the term 'pwned' as originating from the World of Warcraft game, or so the urban legend states. Probably more accurate is that pwned is a misspelling for being "owned," a term used by hackers to signify that they now "own" your computer system and have full access to your data. Not a very comforting thought is it?

We previously wrote an article about securing your data and protecting your computer systems, but this article will deal with what you need to do after a data breach. Certainly the goal is to avoid the data breach in the first place, but we've found most law firms won't spend the money or accept the fact that they are a very vulnerable target. If you've already been compromised, be prepared to spend significantly more money than what you would have spent to prevent the breach in the first place.

The Upchuck Hour

You've just learned that your network has been compromised. What next? The first hour that a security expert spends with you has been called the "upchuck hour" because they have nothing good to say. That's not to say you shouldn't listen. That first hour is used to identify any information concerning the breach. Probably the most important item is whether or not the breach is currently active. If you know there is unauthorized access, should you stop the attack or allow it to continue? As a default action, we would recommend that you take steps to stop the attack and prevent further leakage of data. As a lawyer, you have ethical considerations with respect to your client's data. We'll dig deeper into that later, but stop the bleeding for now.

There may be a rare time when you want to let the breach continue. This would be the case where you need to gather more information about the attackers and the methods they used to gain the unauthorized access. Monitoring the ongoing attack without being discovered is very risky business. You will need highly skilled and specialized experts to accomplish this, which is well beyond the ability of most law firms. Simply pulling the network plug can stop the attack and let you take the next steps in dealing with the data breach.

Preservation and Investigation

The next task is to preserve the appropriate data so that you can investigate the breach and frankly see how much trouble you are in. You may or may not have the skills to properly preserve the data and

more than likely you will obtain the services of security specialists. What should you preserve? That really depends on the attack and where you think the compromise may have occurred. It also depends on the type of data you may hold.

As a minimum, you should preserve any logs from the communication devices and server(s). As an example, all router logs should be captured so you **may** be able to determine the origin of the attack. The server logs should also be preserved. This will help to determine what data may have been accessed. Unfortunately, most servers are not configured for robust logging. We typically find that only basic default logging is enabled. The defaults are short lived and don't capture a significant amount of detailrd information.

PRACTICE TIP… INCREASE THE LOGGING CAPABILITIES FOR YOUR SERVER(S) NOW!

You may need to acquire forensic images of several computers. These could be user computers or the server too. Many data breaches are accomplished by unauthorized personnel that don't want to be found. They will take steps to delete and cover their tracks, hence the requirement for forensic images.

The investigation is important to determine what data may have been accessed, especially if you have data that is subject to any regulatory notifications. Many law firms don't believe they have important data. If you practice family law, think about all the personally identifiable information and financial information (bank accounts, credit cards, assets, etc.) you may possess as part of a case. And if you do estate and trust work – well, need we say more? Also, the investigation may take some time if a large amount of data was preserved and needs to be analyzed. This could impact decisions about data breach notifications, which we'll cover in a bit.

Remediation

Once you know what was accessed and how it was done, it is time to fix the problem. Perhaps the attackers were able to get through to your data because you didn't have the latest patches installed or didn't have adequate malware or virus protection. You may have a router connected to the Internet that is designed for the consumer market and is not intended for business installations. The higher end routers will have better logging abilities and inspect the contents of the data packets in a much more thorough fashion.

Don't think you will be upgrading hardware and software as the only part of the remediation. Policies and procedures will need to be adjusted too. As an example, perhaps you don't require periodic password changes or only require a minimum of 4 characters. A 2010 study by the Georgia Institute of Technology showed that 8 character passwords can be cracked in less than 2 hours. The new standard is 12 character passwords, which would take over 17,000 years to crack with today's computing

technology. If you're lucky, maybe all you really need to do is change your policies to require 12 character passwords instead of the very weak 4 character ones in effect at the time of the breach.

We hope you've been mentally adding up all of the probable costs resulting from the breach to this point. The preservation, investigation and remediation are already totally up to be quite a sum (tens of thousands, even for small firms) and we haven't even addressed the notification requirements.

Notifications

Depending on the type of data that was compromised, you may have legal obligations to notify your clients as well as state and federal authorities. Forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have legislation requiring notification of data breaches. This is in addition to any Federal laws or regulations that may be appropriate for the compromised data. Think you're out of the woods yet? Not so fast. As a lawyer, you also have ethical duties to notify your clients about the data breach even if not required by law.

Don't be like the large New York law firm that refuses to tell its clients that the FBI found their data on servers in China. This was recently disclosed to Alan Paller, the Director of Research for the SANS Institute. Paller interviewed the law firm and walked away with the following quote when asked what they were going to tell their clients. "Are you crazy? Can you think of a better way to destroy their trust in us than letting them know we had lost every document they gave us under (attorney-client) privilege?" The firm made the wrong ethical and legal decision here and we hope the name of the firm will be investigated by the New York State Bar, which can then take appropriate disciplinary action.

As you can image, a data breach can be a public relations nightmare. Just ask the partners at Puckett and Faraj in Alexandria, VA after 3GB of e-mails were obtained by the hacktivist group Anonymous. Not all is gloom though. There are some folks that have prepared for potential data breaches and know how to properly handle the press and potential black eye. The security company RSA was hacked and their very famous SecureID algorithm may have been compromised. While some feel that RSA may have handled the situation poorly, most customers and security professionals applaud RSA's efforts in their quick reaction (pushing out new tokens to customers) and "coming clean" by disclosing their lessons learned from the incident.

The old adage was never more true: An ounce of prevention is worth a pound of cure. So batten down the hatches.

Sharon D. Nelson, Esq. and John W. Simek are the President and Vice President of Sensei Enterprises, Inc., a digital forensics, legal technology and information security firm based in Fairfax, Va. (703) 359-0700 (phone); (703) 357-8434 (fax); sensei@senseient.com; www.senseient.com.