Critical Operations

Why securing your law firm's website is vital to success.

BY SHARON D. NELSON AND JOHN W. SIMEK

One of a law firm's most critical assets is its website and yet protecting it is a priority that is often overlooked. Many lawyers ask why anyone would target them, especially if they are solos or in a small firm. The sad truth is that the majority of attacks against websites are automated. The bad guys throw out a net looking for vulnerabilities and pull in whatever insecure fish they can find—along with any data.

If you are targeted, the risk is much greater. In all likelihood, you are now facing a more sophisticated attacker with a clear agenda who is likely to have more advanced tools. One of the threshold questions is "Where is your website held?" Are you hosting your own website or is someone else hosting it?

For many years, we have advised law firms not to host their own websites. If you do host your own site on your network, all of your data may be compromised if there is a breach. It would be much better to put your website in the hands of another company that has experience in providing security.

Remember that many websites have been taken over by hackers, and the results are never pretty. Your website is your public face. Any compromise of that face, which is generally your primary advertising vehicle, is going to constitute a gut punch to your law firm's reputation.

Sometimes, a hacktivist (a hacker with a political agenda) will redirect your site somewhere else because she doesn't like one of the clients you've represented. Sometimes, hacktivists may try to extort money in exchange for putting things right or for not using the data they were able to harvest.

Many websites collect sought-after information from prospective clients, including email addresses and phone numbers. This all can be sold on the Dark Web. If you have a client portal through your website and it gets breached, the extent of the disaster is compounded exponentially.

Larger websites of big law firms have a considerable amount of computing power at their beck and call. It is possible for a hacker to attack you or someone else with you in the middle of the mess. If you are collecting emails on your website, cybercriminals may use them for phishing purposes, sending messages far and wide in the hopes of compromising someone else.

The problem with a website is that you want everyone to have access to it, which makes it public and vulnerable. If you have applications and interactivity on the website, it is that much more vulnerable because there is code running those functions and custom coding is often riddled with weaknesses. The hacker may be able to submit commands to extract data from your database not in a way that the developer intended. This particular nightmare is known as an SQL injection.

Then there is cross-site scripting, or XSS, in which an attacker uses XSS to inject client-side scripts into web pages viewed by others. The attacker can use XSS to control a web browser and/or modify how content is displayed on a website. You can only imagine the mischief that the attacker can create.

Even the old-fashioned brute force attacks have been known to work. It's a dangerous world and there are now over one billion websites out there waiting to be compromised. Frequently, websites run on open source software and people download vulnerable software. You must be careful to proactively patch your site as security updates become available.

Here's a headline from *Naked Security*: "Critical vulnerabilities pose a serious threat to Joomla sites." The post says "Joomla, the world's second most popular

web content management system (CMS), has been under sustained attack for several days, thanks to a nasty pair of vulnerabilities . . ."

Apparently, flaws in Joomla's user registration code could allow an attacker to "register on a site when registration has been disabled" and then "register ... with elevated privileges." This means that the vulnerabilities could be used to unlock any site running Joomla, anywhere on the internet, with little more than a request detailing what you'd like to be called and how much power you want.

The culprits here were "incorrect use of unfiltered data" and "inadequate checks." We've been reading those words for the past 20 years. The solution, for anyone running an unpatched version of Joomla, is to upgrade to version 3.6.4, which removes the vulnerable code, and then test the website for any indication that it has been compromised.

Sites that run on other types of content management systems can also be impacted. In 2014, more than 100,000 sites using WordPress were hacked. And a heck of a lot of legal websites use WordPress.

So what do you need to do to avoid this morass? You need website vulnerability detection and management. Some website providers offer this, but many do not. There are products that identify and remove malware from your website and firewalls that you can use to block attacks. Tools today tend to be affordable for law firms of any size. Some are even free, though we would be suspicious of their quality.

Everyone would like a security blanket that is 100 percent effective, but "wanting ain't getting" and there is no such thing as 100 percent effective cybersecurity solutions. If a vendor claims to have one, beat a hasty retreat.

So what if the worst happens and your website is compromised? You should be as prepared for a website breach as a breach of your network. You manage the risk in part by simply planning. An incident response plan should cover website breaches and detail the legal authorities to be notified, steps to take to comply with state data breach notification laws, and processes for notifying those whose data may have been compromised.

You have much to gain by building an interactive website with enhancements such as a client portal, but never lose sight of security or you may tarnish your brand's reputation if your site is compromised. Hindsight may not be much of a balm if that happens. **TBJ**

This article has been edited and reprinted with permission.

SHARON D. NELSON and **JOHN W. SIMEK**
are the president and vice president of Sensei Enterprises Inc., a legal technology, information security, and digital forensics firm based in Fairfax, Virginia.