Securing Your Law Firm’s Website: A Critical Cybersecurity Task

by Sharon D. Nelson, Esq. 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. Reading this and you’re not in a law firm? The same rules apply, so keep reading!

A lot of lawyers simply don’t think about protecting their websites. They ask why anyone would target them, especially if they are solos or small law firms. The sad truth is that, today, the majority of attacks against websites are automated. The bad guys throw out a net looking for websites with vulnerabilities and pull in whatever insecure fish they can find – along with any data held on your website.

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 sophisticated 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. Some years ago, one client decided to ignore our advice. The managing partner came to work one day to find that the law firm website home page said "F*** the U.S. Government!" Not precisely the best image for a law firm website!

Also, if you host your own website on your network, ALL of your data may be compromised if the website is breached. Another very unhappy thought. Much better to put the security of your website in the hands of another company which has experience in providing website 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.

So if (yes, it has happened) your website is redirected to a pornography site, you will be tearing your hair out trying to fix the mess. Sometimes, things like this are done because a hackivist (a hacker with a political agenda) doesn’t like one of the clients you've represented. Sometimes, they may try to extort money in exchange for putting things right or for not using the data they were able to harvest.

In this day and age, websites can have a lot of functions. Many collect information from prospective clients, including e-mail addresses, phone numbers, etc. This is information which can be sold on the Dark Web. If you have a client portal through your website and that 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 bad guy to use that power to screw with you, or to attack someone else (with you in the middle of the mess). If indeed you are collecting e-mails on your website, cybercriminals may use those e-mails for phishing purposes, sending messages far and wide in the hopes of compromising someone else.

The problem with websites is that you want everyone to have access to your website which makes it public and vulnerable. If you have a lot of applications and interactivity on the website, it is that much more vulnerable because there is code running those functions, which heightens the possibility that the code has vulnerabilities. Custom coding is often riddled with weaknesses.

Hackers routinely probe websites for vulnerabilities – a weak coding practice by a developer which adds functionality is a potential gold mine. 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 a SQL injection – and boy oh boy, have we seen a lot of those.

Then there is cross-site scripting (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 software that comes with vulnerabilities in it. You must be careful to proactively patch your site as security updates become available.

As we sit typing this article, here is 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 mean 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. And there are millions of vulnerable Joomla sites.

The culprits here were “incorrect use of unfiltered data” and “inadequate checks” – we’ve been reading those words for the last 20 years of web vulnerabilities. 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 their website for any indication that it has been compromised.

How many times have WordPress websites been impacted? A lot, due to the popularity of WordPress. In one 2014 incident, more than 100,000 websites were impacted. And a heck of a lot of legal website 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. There are website firewalls that you can use to block attacks – targeted or not. Tools today tend to be affordable for law firms of any size – some are even free, though we would be suspicious of their quality. To find examples, Google “website malware scanners” and “website firewalls.”

Everyone would like a security blanket that is 100% effective, but “wanting ain’t getting” and there is no such thing as 100% effective cybersecurity solutions. If a vendor claims to have a 100% solution, 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.

In this new era of websites, we are seeing law firms trying to achieve a great interactive experience for their clients. Clients love client portals and love the interactivity, but the more complicated the site and the more interactive it is, the greater the “attack surface” and the more likely the site is to have vulnerabilities making it susceptible to attack. All the neat whiz bang features are wonderful, but you need to work with experts to secure those features. And those wonderful web applications? They (and their custom coding) account for 80% of website vulnerabilities.

We recently had the opportunity to talk with Neill Feather, the President of SiteLock, a firm which specializes in website security in the course of recording a *Digital Detectives* podcast for Legal Talk Network. Disclosure: SiteLock is a sponsor of that podcast. It was a fascinating conversation because we frankly had never interviewed anyone who specialized specifically in website security. To find other such companies, just Google “website security company” – and make sure you get references.

As Neill said, firms continually underestimate the risk of being attacked. He hears them say, “I didn’t know this was something I needed to be worried about.” When we asked him about making a prediction about the future of website security, always a risky proposition, he said (and we agree) that the Internet of Things is revolutionizing security. He expects IoT devices to make website attacks more frequent, with less opportunity to bask in obscurity thinking one is safe. More and more, website owners – law firms included – will need to take proactive steps to protect their websites.

Lawyers tend to view security as an unwelcome chore – and having to deal with website security as well as network security just gives them a monumental headache. But the flip side is to think of website security as enabling. You can do neat stuff with a client portal and other website features giving clients a better experience. This feeds into very successful marketing and ultimately, client satisfaction born of a great website experience.

You have a lot to gain by building an interactive website with a client portal. But never lose sight of security or you may tarnish your brand’s reputation if your website is compromised. Hindsight may not be much of a balm if that happens!

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