Cyber attackers are evolving, are you?

Cyber attackers are constantly searching for new ways to breach your security measures and access the personal data of your firm and its clients. The average hacker is no longer a moody teenager sitting behind a computer. These business-threatening nuisances have evolved into sophisticated networks of individuals and entities who put extraordinary amounts of time and effort into their illegal enterprises – and if you aren't putting a reasonable effort into keeping you client info safe, you may as well hand them your office keys and invite them inside.

Cybersecurity trends

When cybersecurity first became a concern within the legal community, the conversation generally centered on irritating viruses that interrupted the functions of your computing system. Now, the pending threats are much more complex in their workings and malicious in their intent. An article by Ernst & Young likens the current cybersecurity environment to a military arms race, where "cyber threat actors are constantly developing new tactics, techniques and procedures, and businesses are forced to counter these new threats." This dynamic creates a constant tug of war between evolving threats and improved security measures. Straight from the runways of the dark web, let's look at some of the latest trends in cyber threats:

- **Malware as a service.** There is a whole underworld of crime taking place right now on the dark web. (It even sounds scary) Criminals serve as vendors, offering malware services to other criminals. Available options range from malware rental to compete monitoring packages, with commission based payments.

- **Stolen data marketplace.** The dark web is also a hotbed for deals and transactions involving stolen information and data. Entire identities are available to the highest bidder. How would you feel to know that some of this highly personal information originated from your law firm files?
- **Reconnaissance efforts.** According to the Ernst and Young article, these tricky criminals have developed threats that gain entry into your system and sit there for a period of time, exploring and observing your business before transferring desired data from your computers.
- **Increased entry points for attack.** The mobility of the legal community has increased the convenience factor, while also expanding the vulnerability for attack. Smartphones and laptops offer extensive points of entry for cyber attackers. Increased use of internet connected items also fuels this added risk.

An appropriate response

It is clear from these cybersecurity innovations, that your legal practice is up against some formidable opponents. The ABA, along with state bar associations, have issued various opinions regarding your cybersecurity responsibilities as an attorney. So, you should definitely ensure that you are in compliance with these guidelines. What I want to offer is a much more generalized business perspective, based on a widely recognized principle within the cybersecurity community – intelligent decision-making.

It is not enough to blindly implement security measures that may or may not protect your client information. Intelligent decision-making requires an honest view of your current vulnerabilities and strategic planning for your best defense. I know this may sound expensive and burdensome, but think about what could potentially happen. You have an obligation to your profession and your clients to maintain a certain level of cybersecurity. Is this really the most appropriate area for cost-cutting and minimal effort?

About Erika Winston:

Erika Winston is a freelance writer with a passion for law. Through her business, The Legal Writing Studio, she helps legal professionals deliver effective written *messages. Erika is a regular contributor to TimeSolv and a variety of other publications.*