"Our Law Firm is Too Small to be in Danger from Cyberattacks"- WRONG!!!

by Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke

Think Again About the Risks of Small Law Firms

It is astonishing how often we hear small law firms tell us that they are too small to be at serious risk for cyberattacks. Anecdotally, we can certainly tell them of many successful attacks on small law firms, though our knowledge is derived from successful attacks where we've been called in to investigate and/or remediate the damage, so we cannot identify the law firms.

Nevertheless, there are plenty of publicly known small firm breaches. In fact, we have a file cabinet drawer full of articles, reports, etc. of law firm data breaches (small and large) going back 20 years. Why did we build this collection? Because we continually have to persuade law firms, especially the small ones, that they are at risk.

Why Are Small Firms at Great Risk?

For starters, solo and small law firms don't have an exorbitant budget to provide for heavy duty cybersecurity. As a result, they generally rely on their IT provider – which normally does not have cybersecurity certifications – to provide their cybersecurity. As we've said for years…IT is not the same as cybersecurity.

Don't get us wrong – we are not bashing these providers. Many of them are wonderful IT support folks – and they come at an affordable price. And without doubt, all good IT providers know something about cybersecurity. Nonetheless, in the perilous world in which we live, small firms need to up their game with assistance from bona fide cybersecurity professionals.

Yes, some are costly, but there are plenty of affordable small cybersecurity firms – without question, small law firms cannot afford to hire the big firms.

One thing attackers know for sure: Small firms are less protected from attacks – and that makes them desirable (and easy) targets. You may be small, but you still hold the valuable data of many people and small businesses – if you are easy to break into, and criminals armed with your data can then attack your clients, that's a very good payday for them. And just like all businesses, most cybercriminal groups are happy with a certain level of profit – and many of them wish to avoid the increased attention and scrutiny from law enforcement and governments that result from attacks on 'big game' firms.

Small and Mid-size Businesses: Scary Cybersecurity Stats

Recently, we saw statistics from both Accenture's Cost of Cybercrime Study and Ponemon's Institute's State of Cybersecurity Report – and very useful statistics they are. They are not

specific to law firms, but relevant all the same – in fact we would wager that the law firms in general are in worse shape than the normal small/mid-sized business.

Accenture's study found that 43% of cyber attacks are targeted at small businesses, with only 14% prepared to defend themselves.

According to Ponemon Institute's State of Cybersecurity Report, small to medium sized business globally state the following, with respect to cyberattacks:

- Insufficient security measures: 45% say that their processes are ineffective at mitigating attacks.
- Frequency of attacks: 66% have experienced a cyberattack in the past 12 months.
- Background of attacks: 69% say that cyberattacks are becoming more targeted.

The most common types of attacks on small businesses include:

- Phishing/Social Engineering: 57%
- Compromised/Stolen Devices: 33%
- Credential Theft: 30%

The long term costs of a data breach last for months to years and very often they involve significant expenses that entities are not even thinking about or anticipating in their planning.

What might this include? Lost/inaccessible data, business disruption, revenue losses from operational downtime, breach notification costs, legal liability costs and reputational damage. We would add the significant legal costs of hiring a data breach lawyer to oversee the breach response and a digital forensics company to investigate and remediate the breach.

For SMBs of all kinds, legal or otherwise, these statistics should be shared with those in charge of overseeing your cybersecurity. And, for heaven's sake, make sure you have an Incident Response Plan – according to the 2021 ABA Legal Tech Survey, only 36% of law firms have such a plan.

Remember this famous quote from Benjamin Franklin, "Failing to prepare is preparing to fail."

Ethics and Your "Get Out of Jail Free" Card

While lawyers are compelled ethically to safeguard their confidential data and to be competent, including being competent with their use of technology, ethics opinions consistently hold them to a "reasonable" standard.

Two things to bear in mind: What is reasonable for most small firms is less than what would be reasonable for a large firm. Exceptions might include a small but prominent boutique firm or a "Big Solo" firm in which (often) a prominent attorney has a small clientele but the clients may be large and their security needs for their counsel much greater.

The other thing to bear in mind is that what is "reasonable" changes. Today, most cyberinsurance companies regard two-factor authentication, Endpoint Detection and Response software, cybersecurity awareness training for employees, prompt patching of known vulnerabilities, backups which are impervious to cyberattacks and data breach monitoring as "reasonable."

Before you protest that all this is too expensive, 2FA is usually free – and the rest of the requirements can be easily met at a budget-friendly price – you just need to find experts who are not focused on the AmLaw 100 but on serving solo/small law firms.

Final Words

It is often said that "If you can't afford security, you can't afford a breach." And a nod to Sean Connery in *The Untouchables* for his famous quote: "Here endeth the lesson."

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association, and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* *snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional, Certified Ethical Hacker, and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity, and digital forensics services from their Fairfax, Virginia firm.* *jsimek@senseient.com*.

Michael C. Maschke *is the CEO/Director of Cybersecurity of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744), a Certified Ethical Hacker, and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.* *mmaschke@senseient.com*