Article

Cyber Resilience and the Importance of a Plan: How Law Firms Can Defend Against Cybersecurity Risks

11.22.19

Texas Lawyer

World-famous boxer Mike Tyson once said, "Everyone has a plan 'til they get punched in the mouth." Those words of wisdom can pertain tobusiness, life, and in today's tech-driven world, cybersecurity and resiliency.

Many organizations now find themselves completely unprepared for a significant attack and the even greater business disruption it brings. According to the American Bar Association's *Legal Technology Survey Report* (2019), 26 percent of survey respondents said they had experienced some type of data breach at their firm, yet only 19 percent reported they did not know if they had fallen victim to a cyber attack or breach.

The negative consequences of digital security incidents in a law firm can be significant, with loss of billable hours and reputational damage at the top of the list. There are three basic things you can do to help better protect your firm and your clients from the embarrassment and mayhem typically associated with modern-day cyber attacks.

KNOW YOUR BUSINESS AND YOUR RISK

The single most important thing you can do to better protect your firm or business from the chaos and destruction of a cyber attack is simple: know your business and understand the specific risks you face. As an attorney, you spend most of your time trying to understand how to better serve your clients, be more profitable, and perform work at the pinnacle of efficiency. But do you know where your clients' data is kept on your network and can you validate its integrity and security?

Banks have some level of physical currency on hand, which might be enticing for someone to steal, so they typically employ armed security guards and other security measures to protect those assets. Restaurants and retail stores are constant targets of cybercrime as they collect massive amounts of credit card data, so they conduct annual privacy assessments and audits to better identify weaknesses in security and adherence to data protection standards.

But what about law firms? What information might they possess that makes them a high-value target on today's cyber battlefield? Law firms and independent attorneys alike should be aware of three significant areas of data that entice thieves and hackers:

1. **The law firm's own internal data** – This could include the firm's own financial data, client lists and contact information, and firm marketing materials and business plans for managing existing and growing future business.
2. **Data related to the work and representation a law firm provides to its clients** – Communications, particularly emails, between the firm and its clients are desirable. Work product the firm has prepared in conjunction with its representation of its clients, including memos outlining strategies developed for advancing a client's interests, analysis of key legal issues, confidential presentations made to clients, drafts of contracts and other documents prepared by the firm which may contain comments related to confidential communications, intellectual property applications or data related to the fees charged to or collected from a client are also valuable.

3. **Sensitive information the firm has collected related to a client or an opposing party** – Through the discovery process in litigation, a law firm becomes a repository for significant amounts of sensitive business and proprietary information it will end up producing, as well as what's already produced by the other side, and may include a protective order by a court regulating the use and disclosure of this type of information.

These assets can be extremely valuable to common cyber thieves as well as more sophisticated organized criminal operations, and most firms' business networks are left completely unprotected.

BE PROACTIVE

Take a quick glance around your home or office. You likely have physical items and systems in place to notify and protect you in the event of a fire or intruders, including smoke detectors, alarms and fire extinguishers. Likewise, home security and video systems send push notifications when a door or window is opened or if movement is detected in your home, so you feel secure 24/7.

Just as we rely on these types of safety and monitoring systems in our homes, many of the world's largest corporations rely heavily on similar security technology to alert and proactively defend their networks and systems from both external and internal threats. And due to significant advances in modern technology, this type of monitoring is no longer reserved just for Fortune 500 companies.

Proactive 24/7 monitoring by a reputable cybersecurity firm can help your law firm or business easily achieve better security by:

- Scanning and patching your computers and servers for known vulnerabilities and exploits.
- Identifying all computers and devices connected to your network.
- Actively monitoring your cloud and on-premises network for malicious threats.
- Taking swift action based on real-time analysis, often stopping active attacks before they cause significant harm.
- Providing on-site incident investigation and evidence collection and reporting, often negating the need for engaging additional support during times of crisis.

Along with safeguarding your organization from external threats, more robust security monitoring also can better protect your business from malicious actions by internal staff, including intellectual property theft and unauthorized access. Several monitoring solutions also take real-time screenshots and videos of the alleged illicit act and store the materials in an encrypted digital format so they can be used later in HR proceedings or courtroom litigation. Proactive monitoring is an affordable, enterprise-grade level of security that keeps a watchful eye on all your systems and devices around the clock.

Additionally, law firms should put in place measures to control access to data so only the attorneys and staff who need to access specific types of data – or are under similar court-entered protective orders – are given access to only that data. Law firms should avoid putting data onto firm-wide accessible network platforms. Firms also can adopt relatively simple, but highly effective measures, like requiring two-step authentication or six-digit (as opposed to four-digit) access codes before being able to access data remotely.

PREPARE SO YOU DON'T PANIC

Emergency responders and elite military units are some of the world's best students at planning for the worst possible outcome and rehearsing the contingency plan, over and over. Have a plan for how your firm or business will respond to a cyber attack or digital disruption.

Following guidance from the National Institute of Standards and Technology (NIST), some main points of an incident response plan include:

1. **Preparation**

- Are there policies and procedures in place to address a cyber emergency?
- Do you have effective tools and training to handle the incident?

- Communication plans – what is the message you need to send to your clients and employees?

2. Detection

- What security tools are in place to detect an attack?
- Who is in charge of validating the threat and declaring an incident?

3. Containment

- Do you have the ability to identify and isolate the threat?
- Are there procedures in place to address evidence handling?

4. Investigation

- Who will handle the actual investigation into root cause of the incident?
- Are they qualified?

5. Remediation

- Who will handle the repair of affected systems and devices?
- Are there regulatory reporting requirements?
- Do you have qualified personnel who can handle the post-mortem incident reporting and documentation?

6. Recovery

- Who will lead the overall analysis of the incident and incorporate lessons learned into future incident response planning?

With the above framework in place, it also is extremely important to rehearse, or at the very least, make others aware of the plan. Cooler heads will always prevail if everyone in the organization is prepared for the extreme disruption a cyber incident can cause.

Part of having a plan is reviewing the firm's insurance coverages – both malpractice liability policies and general commercial liability policies – to see if their policies cover liability for data breaches. If your coverage doesn't include claims from clients which could arise if the network is breached, or coverage that applies to things like business interruption/disruption which can occur if the firm's email or network systems are compromised, consider purchasing cyber insurance. Some cyber insurance companies offer discounts if you already have strong security protocols or procedures in place.

CYBERSECURITY IS IN YOUR HANDS

Today's business landscape has seen a dramatic shift in just the past 10 years, from how information is stored to how data is monetized. Gone are the days of all client data being printed on reams of paper and housed safely in a banker's box.

To keep up with the pace of their clients and global business trends, modern-day law firms have shifted using digital assets, which comes with notable efficiencies as well as potential pitfalls. Momentum within our tech-savvy world continues, so it is important to become equally cybersecurity-savvy. And remember the human element is always the weakest point in any organization's security model. Education, planning and execution of the plan are key, as we all bear the responsibility of protecting our data and our clients.

The full article can also be viewed by clicking here.

Primary Contacts

Steven Williams
Dallas
214.855.7544
swilliams@munsch.com

Related Practices

Intellectual Property
Intellectual Property Litigation

Related Industries

Technology & Telecommunications