Law Firms and Cyber Attacks â Whatâs a Law Firm to Do? Part One

Cyber attacks targeting the legal industry are a daily occurrence. What is a law firm to do? Part One in this two-part series examines how breaches are affecting law firms, the steps to take, and responsibilities law firms and lawyers must have to help prevent cyber weaknesses. Part Two will focus on communications after a breach, as well as reputation management.

Vivian Hood
Owner/CEO
Public Relations
904.220.1915
vhood@jaffepr.com

Itâs no surprise that the risk posed by cyber attacks and data security vulnerabilities has become one of the top concerns for boards of directors, corporate management, government agencies and the public. There are fast-moving changes in the regulatory landscape, making it even more challenging for everyone to stay on top of compliance and requirements.

Enormous breaches happened in the past year at major corporations of all types, including Under Armour, Uber, Equifax, Verizon, Yahoo and many more. Settlement payments ran into the millions of dollars and, with ever-increasing cleverness by global hackers, there is no expectation this trend will reverse.

How have cyber breaches affected law firms?

Lawyers are not known to be highly sophisticated about technology, and that makes it easy for hackers to get access to information about their clients â whether corporate or individuals. Law firms are being affected by cybersecurity breaches, as just some examples illustrate:

- In March 2016, the FBI warned that hackers were targeting large international law firms; they wanted to steal confidential client information for purposes of insider trading.
- A cyber attack crippled DLA Piperâs operations in June 2017 in a global ransomware event that started internationally and resulted in a preemptive shutdown of the firmâs entire U.S. IT operations for several days.
- A study by the cybersecurity consulting firm LOGICFORCE found that hackers wielding malware prey on vulnerabilities that are âcommonplaceâ throughout the legal industry. âLaw firms should not take comfort in thinking they may be too small or remote to be victimized,â the report warned.
- According to the American Bar Association, 22 percent of more than 4,000 respondents in the 2017 ABA Legal Technology Survey said their firms had experienced a data breach in 2017, up from 14 percent in 2016. Of all survey respondents, 25 percent reported having no policies, with small firms leading in that category, and 7 percent of all respondents said they did not know about security policies.
- In an article in The National Law Journal, one Washington-based firm said the number of attempted daily cyber attacks it witnessed increased 500 percent in just the last two

years.

- Law360 recently reported that â the personal data of up to 1,500 U.S.-based commercial insurance policyholders may have been compromised by a hack at an unnamed â specialist law firm,â according to specialist insurer Hiscox Ltd., and the data breach at the U.S. firm potentially exposed Hiscox customers.
- A new type of cyber attack called â cryptojackingâ hijacks laptops and cellphones, and turns them into unsuspecting cryptocurrency harvesting devices. This should remind attorneys that regulators and lawmakers are finding lax security is not an excuse and to stay on top of emerging threats. New technologies, like cryptocurrency, mean new opportunities for hackers.

Damaging consequences

The ABAâ s survey told of significant consequences to law firms as a result of data hacks, including downtime and loss of billable hours, destruction or loss of files, and having to pay substantial consulting fees for repairing damage that resulted from the attacks â not only the technology damage, but also reputational damage.

Under the ABA rules, a lawyer might lose his or her license over lax data security that leads to a hack of client data.

What is being done to help combat these frequent occurrences?

Since 2017, many cybersecurity regulations passed that require compliance, both nationally and at the state level. For instance, at least 30 states proposed or considered cybersecurity legislation in 2017, and by May 2018, Alabama became the 50th state to enact a data breach notification law. States moved quickly, but the laws are not the same across the board, and it is up to individual lawyers to understand the differences.

The U.S. is not alone. Globally, countries are stepping up on their cybersecurity regulations: Mexico, Russia, China and many more countries have enacted legislation in the past two years, and most recently, the European Unionâ s GDPR became effective May 25.

There is a lot happening, and itâ s all moving fast. In this global world that relies so heavily on technology for communications, it absolutely is critical that a law firm be proactively prepared and protect its clientsâ sensitive data in their systems.

What should a law firm do to be prepared and prevent a cyber breach?

While the largest law firms have made strides in data security, itâ s apparent that mid-size and smaller firms arenâ t making this enough of a priority, as validated by the ABA survey. There are many areas that firms of all sizes must consider.

Hire. Employing a good computer security consultant or vendor to look for weak areas

and provide safeguards is essential, especially if the firm doesnâ▯▯t have internal qualified IT expertise.

Budget. The expense of having robust security measures and planning in place is never going to be as high as the costs of the consequences of a breach in terms of money, time and reputation. Law firms are spending more money this year than ever before for cybersecurity defense, and that line item expense must be budgeted for and expected each year.

Educate. Training of staff and lawyers at the firm on the firmâ▯▯s policies and procedures on preventing cyber attacks is critical, and ideally should be actively discussed or drilled a couple of times per year by the firm. Update the policy at least once annually to stay on top of technology best practices.

Protect. Consider purchasing a cyber liability insurance policy for the firm.

Prepare. Ensure the firm has a crisis communications plan in the event of a breach.

Explain. Law firm clients are paying more attention to how their outside attorneys protect their data. Describe the firmâ▯▯s cybersecurity measures in RFPs and to clients, and make it a differentiator that assures clients they made the right choice in hiring your firm and that their information will be protected. Law firms could face federal regulatory enforcement actions from the Federal Trade Commission if they donâ▯▯t protect client data sufficiently.

Furthermore, Bloomberg Law recently reported that the Corporate Legal Operations Consortium is pushing a new initiative to boost the cybersecurity of law firms while encouraging in-house legal departments to consider their vendors more closely. The group has members from nearly 700 companies representing more than a quarter of Fortune 500 companies, and aims to create a new industry standard.

Update. Updating software, installing security patches and changing passwords regularly, while bothersome, must happen, since those are cornerstones for hackers to access data.

Refresh. Do not overlook what is often the first touchpoint into a law firm: its website. Law firm websites have to follow the most-current and best practices for data security. An outdated website design or lack of a mobile version can raise flags to hackers that a firm may not be diligent about updating security practices, if the website shows they are slack about keeping on top of the latest trends about technology.

What responsibility does an individual lawyer have?

Lawyers didnâ▯▯t go to law school to learn about cybersecurity threats, but they need to know about it now. There are still some lawyers (mostly of a certain generation!) who barely use technology, even email â▯▯ and that makes them especially vulnerable. If the law firm doesnâ▯▯t train in and enforce strict cybersecurity protocols to everyone, these are the lawyers who will unwittingly expose the firm to an attack.

The number one thing a lawyer should do: Become educated about cybersecurity threats

and protection.

A lawyerâ€™s duty of competence includes a duty to be competent not only in the law and its practice but also in technology, since at least 31 states have now made this explicit in their ethics rules. It wonâ€™t be long until it is mandated in every state.

Florida now has a Technology CLE requirement, and Pennsylvania and North Carolina are pursuing similar recommendations. In this new but growing trend, more states are sure to follow.

Resources

- The ABA cybersecurity legal task force website has resources such as handbooks, seminars, reports, programs and more information to help law firms with their cybersecurity needs.
- The Financial Services Information Sharing and Analysis Center is the global financial industry's go-to resource for cyber and physical threat intelligence analysis and sharing. This is a smart information-sharing resource for law firms, pending qualification of membership, and firms can decide on the level of support they need. More than 100 law firms have joined this organization.
- State and national legal associations and groups offer CLE programs, webinars and conference sessions about law firm cybersecurity, prevention and awareness.

Rules, laws and regulations are changing fast, and with entities and hackers who are increasingly sophisticated, the cycle just continues to spin. Lawyers have a responsibility to be current on technology issues on behalf of their clients, and that includes cybersecurity defenses to protect client information as well as their own law firm business.

This article originally appeared on The National Law Review *website on July 17, 2018.*