THE GROWING THREAT TO CYBERSECURITY

By Mark Spitz

In recent years, data privacy has become a serious concern in our increasingly networked world. As more and more personal, health, financial and business data are stored electronically, the security of that data has come under attack from those seeking to steal sensitive information and profit from it. Two highly publicized cyberattacks this year — the "WannaCry" attack in May and the "Peyta" attack in June — infected hundreds of thousands of computers worldwide, targeting governments, hospitals and businesses. One victim of the Peyta attack was the global law firm DLA Piper, which, like other victims, found its computer network and phone system paralyzed. Without access to these resources, employees could not use client files, email or

the phone system for several days, resulting in lost revenue and, given that DLA Piper promotes its cybersecurity practice area, some damage to its reputation as well.

The term "cybersecurity" has crept into our collective consciousness. Cybersecurity is often defined as the set of policies, procedures and technologies employed to protect electronic devices and computer networks from unauthorized access or attack. Cyberattacks against businesses large and small are frequently in the news. Among the better-known incidents are the 2013 attack against Target, which compromised the credit card data of more than 40 million customers, as well as attacks against Sony Pictures, Yahoo and Home Depot. In February 2017, a small Denver car wash business lost its customer records to an attack, and in March, Denver-based Chipotle Mexican Grill suffered a data breach. Hackers sell these customer records to criminals, who, in turn, use them to engage in identity theft, fraud and other illegal activities.

Law firms are no exception to the wave of cyberattacks. In 2016, two large firms, Cravath Swaine & Moore LLP and Weil Gotshal and Manges LLP, were attacked, allegedly by Chinese hackers who sought information on pending acquisitions in order to carry on stock trading before the acquisitions became public.

What, then, should lawyers and law firms be doing to protect themselves and their clients?

While law firms may not maintain customer credit card, bank account or personal health information, as do other businesses, they do have a wealth of data that make them attractive targets. They store data on various types of transactions, corporate structuring, intellectual property, and tax and estate planning — to name a few.

While attacks against large law firms make headlines, smaller firms are at even greater risk. The American Bar Association reported in its 2015 "Legal Technology Survey Report" that law firms with 10 to 49 attorneys were most often attacked, with firms having fewer than 10 attorneys ranked as the next most vulnerable. In 2015, hackers disabled the network of a 10-attorney Rhode Island firm, Moses Afonso Ryan, when one of the firm's attorneys opened an email from an unknown source, allowing malicious software to lock up their network. This resulted in the loss of more than $700,000 in billings over a three-month period because the firm could not gain access to its data, files and records. The firm paid more than $25,000 in "ransom" to get the hackers to decrypt the network and is now in litigation with its insurance carrier over coverage.

The consequences of a breach can be serious and expensive. A 2016 study by the Ponemon Institute, an independent research organization, found that a breach costs an organization an average of $220 per compromised record, which can cripple the resources of a smaller organization. The consequences of a breach can include some or all of the following:

- Potential lawsuits, including class action suits from customers and other affected parties.
- Enforcement actions by federal or state regulatory bodies, such as the Federal Trade Commission for consumer information, Health and Human Services for personal health information, or the Securities and Exchange Commission for public companies.
- Obligation to notify affected customers under state notification statutes, in effect in 48 states, along with paying for credit monitoring services.
- Lost revenue due to lack of access to critical data.
- Cost of rebuilding the compromised network and restoring lost data.
- Damage to reputation and brand.

There is another consequence of data breaches specific to law firms, based upon the Colorado Rules of Professional Conduct. Colo. RPC 1.6(c) obligates a lawyer to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Comment 18 to Colo. RPC 1.6 explains that various factors will help determine if the efforts to prevent inadvertent or unauthorized disclosure are reasonable, including "the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, [and] the cost of employing additional safeguards, the difficulty of implementing the safeguards."

In addition, Colo. RPC 1.1 requires attorneys to provide "competent representation" to clients, and Comment 8 to Colo. RPC 1.1 states that to do so, lawyers must stay familiar with changes in "communications and other relevant technologies." If a lawyer or law firm fails to implement reasonable measures to comply with these professional obligations, resulting in the loss of client information, that could be grounds for discipline. In addition to possible bar discipline, law firms suffering a breach open themselves to malpractice suits from clients.

Why might law firms be vulnerable to hackers? Resources and attention are most often the reason. Many law firms, even larger ones, have not invested enough in their IT systems to make attacks more difficult. They may not see the need to budget for the most up-to-date technology, or may not realize their IT systems do much more than just create and store documents. In addition, widely-used mobile devices such as laptops, tablets, and smartphones are often more vulnerable than in-house systems. Finally, many attorneys are still intimidated by technology and just want to leave things to "the IT guy." However, with the increasing awareness of cybersecurity issues, many clients are starting to evaluate outside law firms' data security preparedness, with some even requiring firms to complete extensive questionnaires. The Association of Corporate Counsel has been

very active in this regard, and developed such a questionnaire. Law firms must be able to respond or risk losing business.

As much as attorneys may believe cybersecurity is just a technology issue, however, it is not. Cybersecurity is an enterprise-wide risk issue and involves much more than IT measures such as firewalls and anti-virus software. What then should lawyers and law firms be doing to protect themselves and their clients? The best approach is a comprehensive one that includes policies, procedures and education in addition to technology solutions. It requires developing a comprehensive cybersecurity plan, which involves doing something that lawyers are already trained in: risk assessment. They need to determine what types of data they hold, the relative importance of the data, the consequences of losing access to it, and applicable laws and regulations.

As part of the risk assessment, a law firm or business may also work with an IT company specializing in cybersecurity, which can identify vulnerabilities in the firm's computer systems and recommend solutions. At that point, the firm can take steps to create an overall cybersecurity plan, which would include policies on system access, password protection, mobile device usage, remote access and incident response — just to name a few. An IT company can assist with implementing recommended upgrades, such as firewalls, malware detection, virtual private networks and network configuration.

Finally, training is critical. An increasing number of breaches now occur as the result of some action, usually unintentional, by an employee. This includes clicking on emails containing malicious software, poor password strength and other actions. Everyone in the firm needs to be trained on how to be a good "cyber citizen," and that training needs to be repeated periodically in order to be effective. Making everyone in your firm aware of good cybersecurity habits is the best way to lower the risk of a breach that could cripple your practice.

Hackers are not going away anytime soon; their methods are getting more sophisticated and change faster than the "good guys" can keep up. There is no way to be 100 percent hack-proof, but law firms and other businesses need to address the issue and take reasonable measures to protect themselves and their client and employee data. D

Mark A. Spitz *is the founder of Spitz Legal Counsel LLC in Denver. He is a former general counsel who works with small and medium-sized companies on transactions, contracts, acquisitions and entity formation. He also advises clients on cybersecurity and data privacy planning and lectures and writes on issues related to data security. He can be reached at mark@spitzlegalcounsel.com.*