The Truth About Law Firm Cyberbreaches Is Stranger Than Fiction

By David Ray and Reggie Pool

This article originally appeared in the National Paralegal Reporter®

During the sixth season of the television legal drama The Good Wife, fictional law firm Florrick, Agos & Lockhart suffered two cyberattacks. The first involved an incident where named partner Diane Lockhart clicked on a PDF attachment in an email purportedly from her colleague Alicia Florrick; however, the email was spoofed. Opening the file launched ransomware that held the firm's computers hostage. Only for a payment of $50,000 was the firm able to get the decryption key, liberate its files, and avoid the permanent erasure of its data. In the second incident, the firm suffered an advanced persistent threat mounted by supporters of a company that the firm had sued. The breach exposed thousands of e-mails from the firm's key partners, airing their dirty laundry. Though the show focused on damage to the partners' relationships and the reputation of newly elected State's Attorney Florrick, the incident seemed to leave the firm's clients unscathed.

Aside from television dramas, law firm cyberbreaches often get little publicity. Unfortunately, the truth is stranger—and certainly harsher—than these attacks on a fictional law firm seem to suggest. For example, in 2002, a paralegal was sentenced to prison after downloading and attempting to sell his law firm's confidential trial strategy plan in a tobacco litigation matter to opposing counsel. In 2010, China-based hackers raided the computer networks of seven Canadian law firms in an attempt to derail an Australian company's acquisition of the world's largest potash producer. And earlier in 2015, a small California firm notified clients that a thief stole a firm member's laptop while he was riding a San Diego trolley.
As these fictional and real-life stories illustrate, the digital security measures of many firms lag behind those of other industries.

Compounding this problem, many firms have yet to fully recognize the risks inherent in their data stores in light of what is at stake. Law firms have a legal and ethical obligation to safeguard their clients' information. Firms that fail to protect their clients' data may face civil liability as well as criminal charges under federal and state law. Breaches can also irreparably damage a firm's reputation. Meanwhile, individual attorneys could be disciplined by their state bar for ethics violations, be subject to government investigations and fines, or face malpractice lawsuits

For these reasons, it is incumbent upon paralegals to understand why their law firms face the risk of cybercrime, learn about potential forms of attack, and take preventive measures to ensure that they reduce the risk of compromising their clients' data.

Why Are Law Firms a Prime Cybercrime Target, and What Are the Risks?

Data is valuable currency—and law firms are stockpiled with it. Hackers view law firms as an appetizing "one-stop shop" by breaching firm security, hackers can access the data of not just one company but also hundreds or even thousands of client organizations at once. In addition, hackers realize that law firms are often behind the curve when it comes to implementing technology to protect their information.

The data law firms store is of extremely high value. Not only is much of it protected by the attorney-client privilege or the work-product doctrine, but it also frequently consists of sensitive commercial information relating to nonpublic business transactions or trade secrets. Law firms also store numerous records sometimes as part of e-discovery repositories for class actions—

that contain personally identifiable information, payment card information, and protected health information, which hackers can often sell for $10 or more per record on the black market.

Moreover, hackers realize that law firms are full of unsophisticated computer users—people who are notoriously slow to implement new technology that can mitigate the risk of data breaches. Some major law firms have begun to address the need to manage their information and appointed chief information officers (CIOs), chief privacy officers (CPOs), and chief information security officers (CISOs), but many smaller firms have yet to adopt a forward-looking approach that recognizes the threats to their digital assets. This attitude shift is unlikely to occur until millennials become sufficiently senior law firm members with the power to influence firm culture and policies.

What Are Common Forms of Cyberattacks on Law Firms?

Though outside hackers receive much media attention, the majority of security breaches are the result of employee inadvertence and misconduct. The BakerHostetler Data Security Incident Response Report 2015 studied 200 incidents and showed that employee negligence and internal theft were responsible for more than half of breaches. Malware and phishing attacks combined for a little more than a quarter of incidents, while outsider theft was responsible for 22%.

Many breaches are attributable to the loss or theft of firm employees' mobile devices. Once obtained, not only can cybercriminals access the data on the devices, but they can also use the users' account credentials to masquerade as firm employees and send malicious messages to other unsuspecting employees or clients. Other common attacks in law firms are spear-phishing attacks, and these are anything but the typical poorly written "Nigerian prince" spam types of messages. Rather, these messages usually target a specific individual within the firm and appear to be from a trusted source, much like the ransomware message sent in The Good Wife, with the goal of accessing account passwords or personal information.

Though outside hackers receive much media attention, the majority of security breaches are the result of employee inadvertance and misconduct. The BakerHostetler Data Security Incident Response Report 2015 studied 200 incidents and showed that employee negligence and internal theft were responsible for more than half of breaches.

Some attacks are political in nature. Foreign governments or other state-sponsored groups may seek to retaliate in response to legal action, or they may simply be engaging in economic espionage. Other groups, such as Anonymous, may hope to make a statement by attacking a particular firm or organization. Insiders with an axe to grind may also choose to retaliate by stealing or misusing sensitive information.

What Can Paralegals Do to Improve Data Security?

As a paralegal, you can take a number of steps to mitigate the risks of data loss.

Limit physical access to client information.

Everyone in a law firm should control access to client files. Instead of leaving sensitive documents visible on your desk, lock them away in cabinets, and do not leave your login credentials accessible in your office. Adhering to a "clean desk" policy – removing not only documents and notes, but any other form of movable information such as memory sticks, sticky notes, etc. – will help reduce your firm's risk of information theft, fraud, or a security breach caused by sensitive information being left unattended and in plain view. Take similar precautions when telecommuting or traveling, including ensuring that others nearby cannot read documents over your shoulder.

Guard client secrets.

Data is most vulnerable when it is in transit. Encrypting files that you send to clients is one way to bolster their security, as it basically encodes every bit of data, making it impossible to intercept without the decryption key. Additionally, take steps to ensure that you do not inadvertently share confidential information online, such as on social media. Avoid using personal e-mail accounts or non-firm sanctioned cloud-based services, such as Box or Dropbox, to send files. When working outside the office, do not use public Wi-Fi, where your online actions can be observed and communications and files can be intercepted. If you receive a suspicious email, contact the sender to confirm the authenticity of the message, and preview any attachments before opening them.

Track client data.

You and your team should carefully track client data from its entry into the firm until its ultimate disposition. The firm should have detailed procedures regarding how to treat data when a matter closes, when a client departs, and when partners or others with primary access to client data leave the firm. Remember – as long as a copy of client information exists, it may be discoverable in another matter, even if the client assumed it was long gone. Once client information is no longer legally required for an active matter, it needs to be returned to normal disposition according to the client's records retention schedule.

Use secure file transfer methods.

We tend to use email for everything – including the transfer of evidence and sensitive information to and from clients. While this may not waive privilege, it nevertheless creates an opening for hackers. Where possible, use secure file transfer tools for social security numbers, payment card information, or other sensitive information. If your firm does not have these tools, ask for them. A number of vendors provide quick and secure tools that are much more secure than email.

Use strong passwords.

Every device you use for any work purpose should be password-protected. Choose a strong password, and do not use the same password for multiple systems. Your passwords should have at least eight characters, consist of multiple character types (uppercase letters, lowercase letters, numbers, and symbols), and not be a common word, phrase, or your name. You should also change your passwords regularly. Password management software can generate strong passwords for you as well as help you avoid the headaches of having to remember unique passwords for every login. Also, set your workstation to log you off after a period of inactivity, so that prying eyes cannot view what you have been working on if you step away from your computer.

Secure equipment.

In the office, prevent thieves from accessing or stealing your computer by securing it to your desk with a lock. Outside the office, keep your mobile devices and digital storage media with you at all times; do not leave them in your car, even if it is locked. Set up tools that enable you to locate your mobile device in the event of theft or loss, and ensure that you have the ability to remotely wipe the data from your devices. Immediately report any lost or missing devices to your supervisor or IT representative.supervisor or IT.

Monitor vendor security.

If client data is sent to outside vendors such as discovery providers, it is important to understand how those vendors manage that information. Make sure that they, too, have appropriate processes for handling client data securely while it is in their hands and returning it to the client or destroying it when a matter has ended.

Stay informed.

Review your firm's policies on data security, computer and device usage, and information governance. Make sure that you do not retain any data longer than necessary under your firm's policies, including its records retention schedules; the more data the firm retains, the greater the risk.

Conclusion.

A law firm is only as secure as its weakest link; therefore, cybersecurity is the responsibility of everyone in the firm. Policies alone cannot prevent breaches; rather, it is the vigilance of every firm employee, including paralegals, that can ensure tales of cyber woe remain just that — a work of fiction — for their firm.

About the Authors

David Ray *is a technologist turned attorney with experience in privacy, information security, records and information management, and eDiscovery. He is currently a director in Consilio's Information Governance and Compliance group, where he helps organizations take a holistic approach to managing their information. He is a member of the Washington State Bar Association and also holds his Certified Information Privacy Professional (CIPP) credentials. He can be reached at:*
dray@consilio.com

Reggie Pool *is a director in Consilio's Information Governance and Compliance Group. He has 24 years of experience consulting in the fields of law and technology. He helps organizations address the rapidly changing requirements of data privacy, security and content control. Reggie earned his Juris Doctor degree at the University of Houston, his Computer Science degree from Texas A&M, and is a Certified Privacy Professional. He can be reached at:*
rpool@consilio.com

This article originally appeared in the Winter 2015 issue of National Paralegal Reporter®.

Consilio®
Together. Stronger.