BY ANDRES HERNANDEZ

Law Firm Cyber-Attacks

How They Happened, What's Next

Cybercrime costs the global economy hundreds of billions of dollars each year. Unfortunately, law firms are not immune to this epidemic.

In fact, the FBI has been warning law firms for years that they are often specifically targeted because they have sensitive and proprietary data that could wreak havoc on the lives of the high-profile clients the firms represent.

And breaches do occur. They happen a lot more than most people realize, because most of them do not go public. Quite the opposite, in fact. They are kept as quiet as possible, because the targeted firms have no desire to let their clients—or their competition—know that they are vulnerable.

ANDRES HERNANDEZ is the co-founder of Wingman Legal Tech, which is a technology consulting firm that specializes in law firm technology. Their technology solutions are designed for simplicity and efficiency.

To put it in raw numbers, one study finds that one in four law firms with more than 100 attorneys has experienced a security breach. And that's on the conservative side. Many other studies actually show the number to be much higher.

Unfortunately, as hackers sharpen their skills and as the knowledge of breaches continues to go unreported, the problem is only getting worse. Yet a majority of attorneys report that their firm has no data-breach response plan in place.

To better illustrate the problem, here are a few stories of recent cyber-attacks that have been perpetrated against law firms, how they occurred, and what happened afterward.

Cyber-Criminal Breaches M&A Deals

The reality of law firm breaches really started to sink in after Cravath, Swaine & Moore revealed they had experienced a security breach in the summer of 2015.

In March 2016, the New York-based firm, which specializes in corporate merger advisory work, became one of the first large law firms to speak to the national press on the matter.

What Happened

An investigation launched around the same time that Cravath spoke to the press discovered that approximately 50 cyber-attacks had been attempted by a Russian cyber-criminal by the name of "Oleras."

Oleras had been hiring people to hack into law firms so he could trade inside information on the black market. Many of these breaches were successful and were kept unknown both to lawyers and to the public until the news about Cravath broke.

The Aftermath

Upon learning about the cyber-attacks, Cravath ramped up security measures and began conducting a thorough investigation, with the help of law enforcement.

Hackers often arbitrarily retrieve a large quantity of data and then analyze it to see what's useful. This can make it hard for investigators to identify what information, if any, was used for insider-trading purposes. At the time that Cravath confirmed the security breach, they mentioned that they could not find any incidents of improper use of stolen information.

Threats From China

In the past, threats of cyber-security have typically come from Russia and Eastern Europe. But an incident at Wiley Rein taught us that China is also starting to launch such attacks on American law firms.

What Happened

In 2012, the Washington firm was handling a trade dispute with a solar panel manufacturer. The dispute led hackers associated with the Chinese military to target the firm.

Later, officials learned that these hackers had been on a huge cyber-attack spree, stealing information from everyone from oilfield services to Canadian magistrates.

The Aftermath

The firm did not share information about the impact of the security breach with the public. But Wiley Rein did promise their clients and employees that the attack encouraged the firm to increase their security efforts. They also hired counsel, Matthew J. Gardner, who is recognized for his cybersecurity expertise.

Your Employees' Safety Matters

Most of the time when law firms beef up their cyber-security, the goal is to protect the personal data of clients and the firm itself. This makes sense. If firm or client data is compromised, it could lead to a mass exodus of clients and cost the business a substantial amount, both in terms of money and reputation.

The actual employees of the firm tend to be of secondary concern. But as international firm McKenna, Long & Aldridge (now merged with Dentons) learned in 2014, bad actors can target these people just as easily, and having employee data stolen is not good for business.

What Happened

In 2014, unauthorized access to a server at McKenna, Long & Aldridge was gained. The cyber-attack resulted in the theft of personal information from many of the firm's employees. Home addresses and Social Security numbers were reportedly stolen.

The Aftermath

Since the breach occurred, the firm has taken a strong stance and made diligent efforts to educate other firms and financial institutions about the dangers of security breaches.

The Threat of Ransomware

Not all hackers commit their crimes in secret, and not all hackers are interested in information. Some are just interested in money. They find a way to break into a firm's cyber data and hold it "hostage" unless the firm pays them a "ransom."

This is a practice that has become more and more prevalent in recent years—so much so that the CBS TV show *The Good Wife* even produced an episode in which the lead actress's firm faced just such a situation.

Here's how a real-life version of that story occurred.

What Happened

In the early months of 2015, California law firm Ziprick & Cramer discovered that a computer had been taken over by Cryptolocker, a form of "ransomware."

This type of software encrypts a computer's data, demanding a ransom before the user can restore his or her information. On many occasions, ransomware schemes have forced law firms to turn over seven-figure sums.

The Aftermath

The firm immediately brought in the FBI and a cyber-attack specialist to assess the situation. The original Cryptolocker virus had affected more than 234,000 computers when the Department of Justice took over the investigation in June 2014.

New versions of the virus began to resurface a few months later. The investigation led experts to believe the virus entered the firm's computer through a phishing email.

After the investigation, the firm announced that they did not believe that any information was used improperly accessed or even downloaded by the hackers. Typically, ransomware attackers are far more interested in getting paid than in getting information.

Although the infected computer did not have a majority of the firm's clients' personal information, Ziprick & Cramer offered clients a free year of credit monitoring to make up for the breach and to allay fears.

The Panama Papers

And now for the big one—in fact, the biggest data breach in the world.

When the Panama Papers were released, the world at large realized that no matter how great your global reputation, as a celebrity, political leader, or law firm, you are still vulnerable to data breaches. Data containing financial deals and other personal information may not be as safe as you think.

What Happened

In April 2016, an anonymous source leaked 11.5 million documents created by the Panamanian law firm Mossack Fonesca.

The documents, some of which dated back to the 1970s, revealed that shell corporations of the firm had allowed individuals, public officials, and organizations to hide money and commit a variety of pseudo-legal and even illegal acts, including fraud and tax evasion.

Not surprisingly, the leak quickly became international news. More than 100 media sources worked together to initially read through and report on the Panama Papers because the amount of data involved was so large—over 2 terabytes.

Because many high-profile figures—from British Prime Minister David Cameron to world soccer star Lionel Messi to famous actor Jackie Chan—appeared in the Panama Papers, it was hard to avoid hearing about the scandal.

At first, the Panama Papers scandal was believed to be a leak from an inside source. Very quickly, however, experts discovered that the release was, in fact, a hack.

Some believe that holes in a WordPress plugin allowed the hacker or hackers to enter into Mossack Fonesca's files. Others place the blame on the firm's email server.

The Aftermath

The hack of Mossack Fonesca shook the world. International outrage forced the Icelandic Prime Minister at the time to resign and many other public officials and individuals mentioned in the leaked papers to stand trial.

Mossack Fonesca co-founder Jurgen Mossack expressed his shock upon learning that associates of Russian President Vladimir Putin and members of China's Communist Party had been involved with the law firm.

And this is an ongoing investigation. Both Mossack Fonesca and its clients are still being exposed in big ways. Recently, the International Consortium of Investigative Journalists reported that new revelations are being made regarding hidden wealth in Africa. The law firm had created offshore companies that catered to businesses in almost every country on the continent. The new revelations show bribery deals and misuse of corporate knowledge by some of Nigeria's and Algeria's biggest names in energy and fuel.

All in all, the data breach was so huge that the investigations and revelations from Mossack Fonesca's files may never be fully resolved.

However, the founders of the firm plan to move forward, increasing security measures and using this horrible incident as a warning to any law firm that holds confidential data, especially data of high-profile and extremely wealthy clients.

Preventing an Attack

Once a law firm truly understands the devastating and costly effects of a cyber-attack, they almost always move forward by creating a strong defense.

This is a great way to prevent such an attack against your firm. But you also should consider taking some precautions before an attack even happens.

Educate your staff.

The more eyes you have looking for signs of a cyber-attack, the better. Communicate with your employees and update them about security best practices as they change. Offer workshops. Send test-phishing emails. Let your staff know that cyber-security is a priority.

Seek outside counsel.

You would likely advise clients to leave law to the lawyers. The same is true with cyber-security; leave it to the security experts.

These people live and breathe hacks and cyber-attacks, and they are able to identify the best ways to defend against them on a daily basis. If your firm does not use outside help or software to monitor the security of your servers, you are leaving yourself exposed and unadvised in the event of an attack.

Develop an emergency response plan.

As already mentioned, most attorneys say their firm doesn't have an emergency cyber-security response plan in place. If that's true of your firm, develop a plan now.

It will require an upfront investment of time and money, but it could save you from much larger, more costly problems down the line. Talk to your lawyers, your staff, and your IT team about what will happen in the event of an attack. And, if any of these measures can be used to prevent a first attack, put them into place immediately.

Utilize DRaaS.

DRaaS stands for Disaster Recovery as a Service, and it should be part of any emergency response plan. The basic idea is that you maintain a copy of all of your data with a third party.

If some kind of disaster ever does strike your firm—natural or man-made—this acts as a failsafe. In other words, if all of the data at your firm is lost, you'll still have that backup data "living" somewhere completely safe, so you can continue to access it remotely and keep your firm up and running.

It is possible to create this on your own without the help of an outside service, but it's costly. Moreover, third parties that specialize in DRaaS understand how to keep that backup data secure because it's what they do.

Just make sure you carefully vet prospective DRaaS service providers to ensure they can meet the defined recovery time and recovery point objectives—or, in plain English, that they can get your needed data quickly and efficiently.

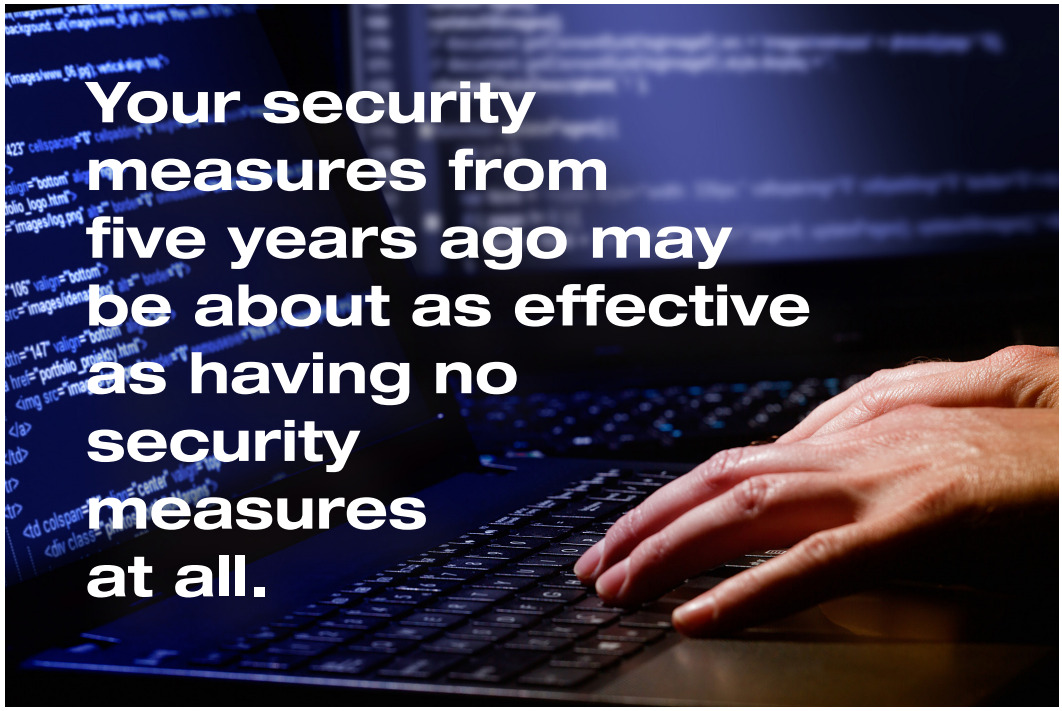
Set up regular penetration tests.

Want to find out how stout your security measures really are? Hire a company like Tevora. Their job, in a nutshell, is to do everything they can to try to hack into your system. Then, when they succeed—and they probably will—they tell you how they did it so you can close that hole in your security.

How good are they? When you hire them, the only information you provide is the name of your company. With their help, you'll quickly learn where your weak links are—and how to shore them up.

Keep updating your systems.

As law firms increase their security measures and find new ways to prevent cyber-attacks, hackers increase their ability to get through those measures and find new



ways to commit such attacks.

Your security measures from five years ago may be about as effective as having no security measures at all. Make security a priority, and continue to increase your defenses.

Install a host intrusion prevention system.

An intrusion prevention system is important, as are any outside measures that will detect foreign access to your computer. Many cloud-based systems have security measures in place that are specifically designed to detect and stop suspicious foreign access.

Host intrusion prevention systems will run every time you turn on your computer, analyzing events within the computer and alerting you of suspicious activity. It is a great addition to installing firewalls and putting other security measures in place.

Conclusion

The bottom line is that cyber-attacks not only happen, they're occurring more frequently. And perpetrators are growing increasingly bold.

Regardless of the size, security, or knowledge of your firm, you are still at risk of a cyber-attack. Educate your employees. Beef up your security measures. And communicate and report any cyber-attacks that do occur to keep everyone aware. AZ AT