THE
NATIONAL LAW REVIEW

Cybersecurity: Law Firm Data Breach come in Different Forms

Thursday, February 28, 2019

Hacking doesn't just happen to governments in *Mission Impossible* films anymore. Hackers don't only focus on getting passwords and credit card information from unsuspecting consumers online either. Law firms are big business in the hacking world now, too. According to the American Bar Association, one out of every four law firms is a victim of data breach. That is a staggering figure: 25% of all law firms practicing in the United States alone have experienced at least one data breach.

Many want to know what can be done to prevent this, of course. The best way to defend yourself, some have said, is to know the enemy. In the spirit of that advice, it is important to get a sense of the different kinds of data breach that can occur, how they are happening, and who is perpetrating them on law firms' servers and accounts.

There are five, unfortunately, "common" types of data breach attempts on practicing law firms: inside information, hostage and ransom, user error, surveillance, and even hacktivism. Each one is worth considering on its own.

Article By PracticePanther
Jaliz Maldonado Practice Panther

Communications, Media & Internet
Law Office Management
All Federal

Inside Info – A data breach from the inside out.

It is common knowledge that attorneys must hold onto an incredible amount of information. As technology has progressed, paper has become less and less utilized as a form of record-keeping. While some information is still recorded and stored on paper, even those documents are often transferred to a digital scan, so that it exists in a data format as well.

Some of this data is likely to contain information about businesses and their practices and dealings, contracts and the like. As such, nefarious individuals and organizations would love nothing more than to their digital paws all over it. If they can access this data, they might get ahold of merger info or confidential acquisition details before they are made available to the public. This ultimately leads to insider trading.

Ransomware – The devastating click or download.

This particular kind of hacking has been around for some time, but it has grown in popularity within the last few years. The way it works is relatively simple, but it has devastating consequences. A hacker gets an attorney to install a program on their computer (via an official-looking email or link online). That application is actually a covert program that takes over the lawyer's machine, disabling the system and thereby holding the files and data hostage.

Once they have the computer in their clutches, the hacker will demand a certain amount of money. They either request to be paid directly in an attempt to further steal by confiscating the person's identity information, or they demand an untraceable format, such as Bitcoin or other cryptocurrencies. Once the payment has been made, the

hacker releases the computer back to the attorney (in theory). While the information may never actually leave the server or computer in question, it can render a lawyer's technology useless until the problem is resolved.

User Error – The accidental post or email

One of the worst forms of data breach is also perhaps the least exciting. Sometimes, all it takes for information to be leaked or lost is a simple mistake. People make mistakes all the time, but ones involving law firm data can be incredibly costly and even result in legal action. It can be as innocuous as accidentally sending a confidential document to the wrong email address or not encrypting emails as they are sent and received.

Human error through email or website links can also result in ransomware attacks, as detailed above, or in phishing attacks, where login information is input and subsequently stolen, which can result in insider information also being lost.

Cyber Surveillance – The data breach that watches.

It isn't quite *1984*, but it might as well be when it comes to digital espionage. This is related to the phishing attacks previously mentioned under user error. Hackers or digital surveillance organizations typically attempt to bait users (attorneys, paralegals, executive assistants, etc.) with an official-looking email. It asks the user to log in to what appears to be an official website. Of course, it isn't, but once the login has been performed, the damage is done.

The hackers now have the individual's login information and can access anything that the person himself or herself has access to on their servers. This can include confidential information, entire email databases, contracts, private and personal information, financial records, etc. The list is virtually endless, and it can breach attorney-client privilege, as any of these others can as well.

Hacktivism – The information leak of data breaches.

Unlike the others, political hacking (or hacktivism, as it is commonly known) is not usually financially motivated. Rather, these hackers have political or socio-political aspirations in mind. Arguably, the most notable instance of hacktivism is the Panama Papers, in which more than 11 million documents were leaked from the Panamanian law firm Mossack Fonseca in 2015.

The source of the hacking was anonymous, but the information they released most certainly was not. The Panama Papers revealed comprehensive financial documentation and breached attorney-client privilege for over 200,000 entities located offshore, many of them incredibly wealthy individuals attempting to keep their financial dealings and records private.

Last Notes

Whether it is accessed via human error or direct hacking attempts, and whether the goal is financially or politically motivated, hacking affects more law firms each year. Keeping in mind the scope and possibilities of the attacks themselves will hopefully encourage more attorneys in the United States to be proactive, and educate partners and other employees on best and safe practices for online information and the transmission thereof.

Source URL: https://www.natlawreview.com/article/cybersecurity-law-firm-data-breach-come-different-forms