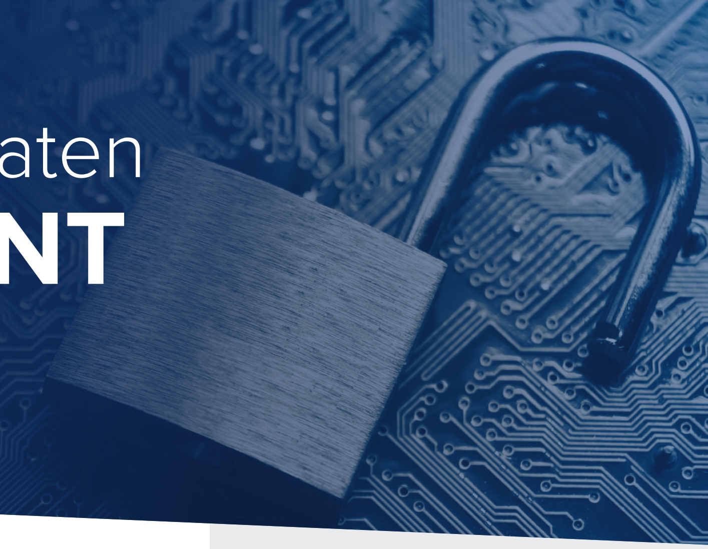

Security breaches threaten SENSITIVE CLIENT INFORMATION

Unfortunately, despite the good intentions, law firms represent an easy target for attackers due to a generally weak security posture. Researchers estimate that 93% of law firms have been hacked and the remaining 7% just don't know it yet.

(Source: McAfee, Information Security Magazine)

Recent Cybersecurity Incidents Involving Law Firms

The Paradise Papers

On Nov. 5, 2017, the International Consortium of Investigative Journalists published 520,000 entries based on 13.4 million records from a 2016 breach at Bermuda-based law firm, Appleby. Branded as "The Paradise Papers," those records exposed how high-profile companies such as Apple, Nike and Uber, as well as Bono, Queen Elizabeth II and Madonna, used the firm's offshore taxation expertise. In an official statement from the firm on Nov. 6, "Our systems were accessed by an intruder who deployed the tactics of a professional hacker and covered his/her tracks to the extent that a forensic investigation by a leading international Cyber & Threats team concluded that there was no definitive evidence that any data had left our systems."

DLA Piper

In June 2017, a massive attack on DLA Piper, forced the global law firm to shut down its IT functions. For nearly a week, the firm's phones and email systems were down, with attorneys and staff instructed to communicate via text and cell-phone calls. On July 7th, the American Lawyer reported that the firm was still struggling to recover from the attack, and that the fallout could cost "millions." Clearly, this incident will be remembered as a cautionary tale for the legal industry with regard to the impact of a cyber breach.

The Panama Papers

This was an unprecedented "leak" of more than 11 million documents/files spanning over four decades, from the Panamanian law firm, Mossack Fonseca. That firm is reportedly the fourth largest "offshore" law firm, which helps establish secret shell companies and offshore accounts and companies for global power players. Among other items of note, the documents revealed the names of world leaders who have established offshore tax havens.

Cravath/Weil

On March 29, 2016, the Wall Street Journal reported that hackers had broken into the files of some of the biggest law firms in an insider-trading scheme that involved planned mergers. Although the Manhattan U.S. attorney's press release didn't name the firms, news media matched details in the release to law firms that represented parties in the mergers and named Cravath, Swaine & Moore and Weil Gotshal & Manges as being victims of the hack.

Oleras

"Oleras" targeted 48 law firms. It was recently discovered that a Russian cybercriminal named "Oleras" and his/her gang had targeted 48 of the nation's most prestigious law firms to try to steal confidential client information for insider trading. The plan, according to firm Flashpoint, was to infiltrate the law firms' networks, use keywords to obtain drafts of merger agreements, confidentiality agreements and trading activities, and then engage in insider trading.

Anatomy of a RANSOMWARE ATTACK

Initial Infection

Ransomware infection typically happens when an unsuspecting user clicks on a link or opens an infected attachment in an email correspondence.

The Spread

Once on a host, the ransomware searches the system for files to encrypt. Some forms of ransomware will also spread to mapped network drives.

Data Encryption

Encryption of data, documents or the operationed system can take place instantaneously, making them inaccessible to the user.

Message Displayed

A ransom screen instructs the user how much time they have to pay a fine in return for a decryption key. In the event of a non-payment, the ransom fee increases or files/systems are destroyed.

BLUVECTOR®

STAY AHEAD OF THE THREAT. BluVector has reinvented the network intrusion detection system with patented machine learning and speculative execution engines so that it can finally defend the network against even the newest and most sophisticated cyberattacks.

Before your next breach, visit **www.bluvector.io**