ANATOMY OF A RANSOMWARE ATTACK
Who is at Risk for a Ransomware Attack?

More than 30 percent of businesses experienced a ransomware attack in the past year—with 22 percent of those organizations forced to immediately cease operations to deal with the fallout.

This is sobering news, and it lays bare a simple fact: Ransomware and other types of malware—often delivered via “phishing” attacks, innocent-looking emails that can infect users’ computers—aren’t isolated to a single country or geographic region.

But how vulnerable is the legal community? According to NTT Security’s 2017 Global Threat Intelligence Report, four industry sectors absorbed the brunt of attacks worldwide: business and professional services (28 percent), government (19 percent), health care (15 percent) and retail (15 percent). Legal falls squarely under “business and professional services,” meaning the threat to the industry is very real.

For one, law firms and legal departments deal almost exclusively with confidential matters like sensitive intellectual property, trade secrets and mergers and acquisitions. And plaintiffs’ firms handle extremely confidential information about their clients’ health: it’s a routine part of the job to deal with personally identifiable information (PII).

Regardless of the practice area, law firms create and modify thousands of documents per day amid time-sensitive issues and court-ordered deadlines. This makes them ripe targets for ransomware attacks.

By 2021, global cybercrime is predicted to cost $6 trillion. This includes costs related to damage and destruction of data, stolen money, theft of intellectual property and personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, and reputational harm.

Yet the industry is barely taking notice: Only 8.4 percent of attorneys named cybersecurity risks as a top concern, while increasing revenues ranked far higher, at 20.9 percent. And according to LogicForce’s Q1 2017 Law Firm Cyber Security Scorecard, 53 percent of law firms have no data breach incident response plan in place, while some 77 percent don’t even maintain cyber insurance coverage.

These facts and figures paint a nerve-wracking picture of just how exposed the industry is, and how much it needs to prepare for the inevitable. But client pressure is beginning to force the issue: the 2016 ABA Legal Technology Survey Report found that nearly 31 percent of all law firms and close to 63 percent of law firms with 500-plus lawyers said that current and potential clients require them to have robust cybersecurity plans in place.

In terms of preparation, it starts with daily on-and-offsite data backups that are routinely tested for security flaws. Employee training is also critical; since ransomware usually spreads via infected email attachments, enterprise-wide best practices in email awareness can help mitigate the threat.

Law firms can also move to the private cloud, which enjoys robust security features that often outpace firms’ in-house capabilities. Most cybersecurity experts agree that the private cloud provides high levels of control and security—ideal for the legal industry and its sensitive information.

The Mechanics of Ransomware

Ransomware, by definition, is a piece of malicious software (malware), that, once unleashed via the
click of an infected email or attachment, blocks access to a computer's files until money is paid to unlock them.

“Ransoms” are often demanded in bitcoin or other online currency, and can range from a few hundred dollars into the tens of thousands and more. A recent example is WannaCry, which captured the world's attention earlier this year when it spread rapidly across the globe, affecting hundreds of thousands of machines and crippling businesses as they struggled to recover.

But what, exactly, happens in a ransomware attack? In a typical scenario, an end user—say, a clerk at a mid-sized law firm—receives an apparently legitimate email from his or her supervisor. It directs the clerk to a website containing software called an “exploit kit,” which, as the name suggests, is designed to exploit a computer's vulnerabilities.

According to cybersecurity firm Carbon Black, once that web page is loaded, the server hosting the exploit kit communicates with the user's computer to find vulnerable software. The malicious file then executes on the victim's computer, encrypting its files and replicating itself so it can restart at each subsequent login or reboot.

Once the victim's files are encrypted, the encryption key is sent back to the server, which then prompts a ransom message to appear on the user's screen. Victims can only access the encryption key by paying the demanded ransom.

Indeed, as far as ransomware goes, the encrypting kind is about as bad as it gets, and is usually spread by infected email attachments that users click. However, it should be noted that WannaCry spread with no user interface (i.e., clicking on a malicious email attachment), but rather via a so-called “ransomworm” that searches for vulnerable public-facing Server Message Block (SMB) ports, using various exploits to get on networks and propagate from there. Indeed, many media reports inaccurately portrayed WannaCry as being introduced via phishing, when in reality, an email scam had nothing to do with it.

The History of Ransomware

It is generally accepted that the first known ransomware attack happened in 1989 and was initiated by an AIDS researcher who, at a conference, distributed 20,000 floppy disks to colleagues from more than 90 countries. Also known as the PC Cyborg virus, the AIDS Trojan ransomware lay dormant on a user's computer until the machine was booted 90 times, after which the malware would lock the files on its hard drive. Users had to send $189 to a PO Box in Panama in order to regain access to the files.

Malware and ransomware has grown significantly more sophisticated since those early days, with industry experts pointing to 2005 as the year that the first waves of encrypting ransomware began to hit. Trojan.Gpcoder arrived in May 2005, according to a paper published by Symantec, using “symmetric encryption algorithms, which meant the same key was used for both encryption and decryption.”

The paper points out that the next pivotal moment in ransomware happened in 2008-09 with the advent of fake antivirus programs which copied the “appearance and functionality of legitimate security software.” The difference? The programs claimed to find major security issues on a victim's computer, demanding small fees to repair the problems. Then, in 2011, there was a shift to locker ransomware and eventually encrypting ransomware, which is currently the method of

www.abacusnext.com
choice to extort money from its victims. It doesn't end there, however. A new form of malware is cropping up that is designed to destroy files altogether (think “Petya” or “NotPetya”).

Now What?

Given its history—and the fact that ransomware and other types of malware will no doubt continue to grow in sophistication—law firms and other companies would be well served to have a plan in place for what to do in the immediate aftermath of an attack. For firms carrying cyber liability insurance, the first thing to do is notify the insurer and trigger the policy. If no cyber insurance is held—and the majority of law firms do not carry such policies—the next step is to immediately notify the appropriate IT personnel. In the best case scenario, firms can then restore their data from an offsite or cloud backup (even as productivity slows or even stops altogether). But if the backup is also encrypted, choices rapidly dwindle from there. What remains? Pay the ransom, receive the encryption key—and pray that it works.

There are, however, silver linings associated with these nightmare scenarios. One, knowledge (and preparation) is power. Firms unlucky enough to fall victim to a ransomware attack will likely never find themselves in the same situation. For firms that simply read about attacks in the news and take protective actions and steps, the key is to be ready.