Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

5 Things To Know About Ransomware Attacks

By **Allison Grande**

Law360, New York (June 28, 2017, 3:17 PM EDT) -- This week's global cyberattack, like one in May that held 300,000 computer systems around the world captive for days, is among the worst ransomware intrusions to date and likely not the last of its kind. Attorneys say that being prepared and knowing the steps to take in the wake of an attack could help reduce legal exposure and public scrutiny.

The so-called Petya attack on Tuesday and the WannaCry attack on May 12 locked the data of government entities and global businesses, including DLA Piper, by encrypting their files — or whole systems — and holding them hostage in exchange for a ransom payment. The May event first turned experts' attention to a devastating ransomware method that was used again Tuesday and that attorneys say is gaining currency among a global, highly organized set of hackers.

"Gone are the quaint days when hackers wanted your credit card number," said Brenda Sharton, a Goodwin Procter LLP litigation partner and chair of its privacy and cybersecurity practice. "Now it is about content, corporate espionage, and the hackers are nation states and organized crime."

Experts in cybersecurity shared with Law360 advice for what businesses should do to not only guard against an attack but also how to respond if hackers succeed at seizing their data.

No One Is Immune

The Petya and WannaCry attacks seized data in systems in more than 150 countries, but the intrusions are also astounding for the sheer number of industries they have hit.

Lisa Sotto, who heads Hunton & Williams LLP's privacy and data security practice, discussed the May hack using WannaCry malware as among the first of a bold new breed of worldwide attacks and a precursor of more devastating future attacks.

"The extraordinary global reach of WannaCry and viral nature of the malware as it spread across the globe was both frightening and entirely predictable — and a harbinger of things to come," Sotto said.

Despite their vast impact, the Petya and WannaCry attacks shared many similarities with recent ransomware attacks that have hit hospitals, banks and other institutions, incidents that hint at a rising class of hackers who seek targets most likely to meet their demands, attorneys say.

"Ransomware attacks are definitely up to be sure, and an objective review of the statistics shows that it's up relatively significantly," said Paul Rosen, a partner with Crowell & Moring LLP and a former chief of staff at the U.S. Department of Homeland Security. "So it's something that businesses are going to really need to focus on."

FBI statistics show that ransomware attacks quadrupled, jumping from 1,000 a day in 2015 to a daily 4,000 detected intrusions in 2016. The numbers are expected to continue to rise this year.

Data breach response insurer Beazley Group backed up these figures in a report earlier this year that revealed that the number of ransomware attacks among its entire client base in 2016 was four times higher than the previous year and that these incidents had spelled significant trouble for businesses in the financial services, retail, education and hospitality sectors, which saw the highest rates of attack.

Similarly, BakerHostetler reported in its 2017 data security incident response report that of the more than 450 cyber incidents it handled last year, 10 percent involved ransomware. It also said that "while ransomware has existed in one form or another since 1989, the past two years have seen a tremendous increase in the frequency and variety of attacks," with some researchers having observed an up to 500 percent year-over-year increase in ransomware incidents.

Law firms are an enticing target. Bill Hardin, a data breach and cybersecurity expert at consulting firm Charles River Associates, said during a conference in March that the sensitive client information retained by law firms is an attractive mark for cybercriminals and that firms should be wary of the threat of ransomware attacks.

"It's an absolute arms race between the hackers and companies," Sharton said. "And these attacks are only going to continue to increase in frequency and sophistication. We're definitely not dealing with your grandfather's breaches anymore."

Precautions Can Be Taken

One factor that attorneys say potentially contributes to the swell of ransomware attacks is that it’s easy for hackers to collect big paydays while exerting little effort.

"A ransomware attack is relatively easy to commit with little chance of being caught," Sotto said by email. "Attackers make money fast, without having to go through the extra step of having to sell stolen data to make a buck (or a bitcoin)."

Attorneys advise taking relatively simple steps to make the hacker’s job harder: Patch known vulnerabilities, run the most updated systems, educate employees about phishing emails that hackers often use to gain access to corporate networks, and back up vital data.

"Preparing for ransomware attacks needs to be part of a business's overall security regime," Rosen said. "Just like you close your windows and doors before you leave home and don't leave a spare key under your front mat, taking basic measures to safeguard your data and network could go a long way."

Both the Petya and WannaCry attacks were carried out by hackers who sent out phishing emails with malware that exploited a vulnerability in the Windows operating system. The malware apparently had been created by the National Security Agency to investigate external threats to the U.S. Microsoft had issued a patch two months before the attack took place, highlighting the importance of taking these basic security precautions.

"Leaving software unpatched creates a security hole that a Mack truck can drive through," Sharton said. "And malware that gets into computers through phishing emails is getting more sophisticated and realistic now, which makes it even more important that companies do constant training and give constant reminders to employees to be careful about what they're clicking on."

Tough Choices Loom About Payment

Even if companies do take basic security precautions, determined, sophisticated hackers will take advantage of any lapse in defenses, and attacks still will succeed. If an attack occurs, should businesses pay the ransom of a few hundred to perhaps several thousands of dollars, or is there another way?

"If the impacted company has backups of its systems and data, it can restore its network without paying the ransom," Sotto said. "The unfortunate reality is that many companies do not have sufficient backups — so they have no choice but to pay the ransom in order to continue operating."

A company deciding whether to pay a ransom, among other things, must assess the adequacy of data backup, judge the sensitivity of threatened information and gauge the effects of a lockout on the company's operation, attorneys said.

Although the FBI spoke out against paying ransoms in an April 2016 bulletin, companies still pay up especially if the sum is relatively small. In the case of both the Petya and WannaCry attacks, the hackers demanded $300 in exchange for the decryption key. The amount of ransom paid to the Petya hackers hasn't been calculated, but security researchers estimated the attackers collected about 15 bitcoins — or about $26,148 at the current bitcoin-to-dollars exchange rate — in the first day after the WannaCry attack.

Other businesses have elected to pay higher ransoms in smaller ransomware attacks, including a $17,000 ransom that Hollywood Presbyterian Medical Center paid in bitcoins last year to get back online. South Korean web hosting company Nayana also agreed earlier this month to pay a hefty $1 million ransom, after negotiating with hackers who had originally demanded around $1.6 million.

"Not all companies have the luxury of rejecting the attacker's demands because their files are locked up with no hope of recovering them if they fail to pay," Sotto said.

Continuing to pay ransoms, however, may spur hackers to step up attacks, attorneys said.

In its 2016 bulletin, the FBI said that "paying a ransom doesn't guarantee an organization that it will get its data back — we've seen cases where organizations never got a decryption key after having paid the ransom." The bulletin added that giving into the hackers' payment demands "not only emboldens current cybercriminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity."

Attorneys agreed that as long as the hackers are paid ransom, the attacks are unlikely to lose steam.

"When it comes to a ransomware attack, the question is, 'How easy is it for these actors to conduct the cyberattack? What's the cost for them of conducting the cyberattack, and are their costs going to go up or down?'" Rosen said. "If ransomware remains very cheap for hackers to launch and they keep getting paid and are not being held accountable, then it's a low-cost proposition. But if they're not getting paid and the government is putting the hackers in jail, that's a much more high-cost endeavor."

You May Want to Call Law Enforcement

When responding to a ransomware attack, attorneys advise that companies should at least give some consideration to what role the FBI or other law enforcement agency could play to help companies recover from the attack and hold the hackers accountable for their actions.

"Any type of attack where somebody is in your network and actively ransoming your data, law enforcement can likely assist both in the immediate, as well as in terms of going after bad actors in a way private citizens and companies cannot," Rosen said.

As with paying ransoms, deciding whether to alert law enforcement depends on the specific facts of the situation. While companies may be hesitant to open up to law enforcement for fear of losing control of the response efforts and revealing too much information, the move could have some advantages, attorneys said.

"If you are dealing with regulatory enforcement from another branch of the government, it may be advantageous that you've tried to involve law enforcement from the get-go," Sharton said. "It also may be reassuring to customers and help reputationally to show customers that law enforcement has been notified and is trying to get to the bottom of it as well."

While not all companies may choose to call law enforcement, attorneys recommend that when ransomware is discovered, companies should retain some sort of experts to assist them with unraveling the mess that the hackers have left.

"Too many companies try to go it alone," Sotto said. "It’s important to call an expert so the attacker's footprints are not destroyed in the process of attempting to remediate the problem."

Standard Breach Reporting Obligations May Apply

While targets of ransomware attacks may get their data back before it's exposed or misused, the company's breach reporting obligations under state and federal laws, in most circumstances, still apply.

"One of the things that comes up in the wake of ransomware attacks is that companies want to know if they have to notify," Sharton said. "Even though most of the time, hackers free the database and don't mine the information, companies still have to assume unauthorized persons accessed the information, and unless they're able to tell through forensics that they haven't, they have to notify."

The U.S. Department of Health and Human Services' Office for Civil Rights has made it clear that a ransomware attack that affects protected health information is a "security incident" under the Health Insurance Portability and Accountability Act, Sotto said. Unless the health care provider or business associate can demonstrate a "low probability" that personal health information was compromised, a reportable breach is presumed to have occurred, she said.

Breach reporting laws in place in 48 U.S. states may also trigger notification obligations, although if the data is encrypted or locked up through an automated process, companies may argue that it was not accessed by an unauthorized party, which is the standard that typically triggers breach notification laws, Sotto added.

"Dealing with the fallout of an attack means that a company has to know what notification requirements it has to the government, the state and elsewhere," Rosen said.

--Editing by Christine Chun and Katherine Rautenberg.