Ransomware as a Data Breach: An Evolving Threat

by Sharon D. Nelson, Esq. and John W. Simek

It is hard to believe there was such a thing as "the good old days of ransomware," but we might be forgiven for looking back nostalgically. While ransomware was a bloody nuisance, law firms generally felt protected if they had a well-engineered backup system to facilitate recovery.

With multiple backups, usually in the cloud, or (with small firms) on two or more external USB drives, you could ignore the badgering requests to pay the ransom, the clocks counting down to when your data would be totally inaccessible, etc.

The trick was always to have multiple backups so that a single backup solution didn't leave you vulnerable to having all your data encrypted if you were struck by ransomware while backing up. Having that "virgin" backup meant you could restore the data. This of course assumes that you regularly performed test restores on your backups to make sure you could indeed restore data from them.

Good guys, 1 — bad guys, 0.

The exception was often in the health-care industry, where lives were at stake and taking the time required to restore data might cost lives. Often, those entities paid up—and once the cybercriminal discovered that, health-care entities were targeted.

If you are scratching your head about all the state and city governments that were brought to their knees by ransomware in the last two years, you should know that their backups were not properly engineered. In fact, they were a mess. The cleanup took forever and cost millions of dollars. Many local and state government agencies never understood what constituted properly engineered backups—nor did they budget for it. Even now, they are more likely to get cyber insurance to cover the risk than to adequately address the baseline problems.

Cyber Incidents vs. Data Breaches

Fast-forward to December 2019 when ransomware gangs upped their game and began to threaten that they would "out" the data of those hit by ransomware if they didn't pay the ransom.

That altered the previous rules of engagement—and it meant that they had exfiltrated (taken) the data before encrypting it.

Previously, it was generally safe to say that ransomware attacks were only rarely data breaches—mostly they were cyber incidents. Your data was encrypted but not exfiltrated. What did that mean? You didn't need to report those incidents under state data breach laws or under many other laws/regulations.

Innocent days indeed. Ransomware cybercriminals are upping their game—some say they will begin publishing data taken from entities that don't pay the ransom. To the horror of victims, one ransomware gang now has a public website naming entities that have restored their data and reconstructed their systems instead of paying the ransom. For the moment, information given for each Maze victim comprises the date of infection, the size of files supposedly taken from victims (in gigabytes) and a handful of stolen Microsoft Office, text and PDF files. Also identified are the IP addresses and machine names of the Maze-infected servers.

In fractured English, the site says, "Represented here companies don't wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news!"

Yes, indeed, we will be continuing to follow the news. If the Maze tactic is successful, this is very bad news for law firms, which have almost invariably regarded ransomware infections as a security incident and not a breach.

Did We Have Warning of this New Ransomware Tactic?

From our foxhole, the strictly correct answer is no. Until the recent news broke, we had not heard a specific case of data being exfiltrated. But we had thought about it. It seemed logical to us that bad guys who would demand ransomware to get your encrypted data back would be very likely to take your data before encrypting it.

There is, after all, no great honor among thieves. We ultimately concluded that the only thing stopping them from taking data (as an insurance policy for getting payment, if nothing else) was if the exfiltration could be traced. And there's the rub—maybe it could be traced, maybe not. But we fretted over it—and thought that the smarter cybercriminals might indeed be able to erase their tracks.

Law firms were happy to hang their hat on the most convenient nail—and that meant that there was no evidence of data compromise (but did they look for evidence?) and they didn't need to report data breaches. Convenient thinking, but in light of the new threats, we believe law firms need to take ransomware much more seriously than they have in the past. Frankly, many law firms do have well-engineered backups and could return to full functionality fairly quickly after a ransomware infection. And that's where they wanted the story to end.

It appears we should have worried more. Lawrence Abrams, founder of the computer security blog and victim assistance site BleepingComputer.com, recently said in his blog that the bad guys have warned us about this problem: "For years, ransomware developers and affiliates have been telling victims that they must pay the ransom or stolen data would be publicly released. While it has been a well-known secret that ransomware actors snoop through victims' data, and in many cases steal it before the data is encrypted, they never actually carried out their threats of releasing it."

Well, it wasn't a well-known secret to us or to many of our colleagues. But OK, let's start from where we are today.

Does Your Law Firm Have a Managed IT Services Provider?

It gives us no pleasure, as a managed IT services provider (MSP) ourselves, to report that MSPs are being targeted by ransomware groups. MSP Synoptek was hit in late December 2019, with many of its more than 1,000 customers having their services disrupted. The company has reportedly paid a ransom in an attempt to restore services as quickly as possible.

In October 2019, law firms using cloud-based TrialWorks case management software lost access to their legal documents for four days after TrialWorks was hit with a ransomware attack. Several of our friends were near hysteria, severely crippled by the inability to do their jobs.

TrialWorks serves roughly 2,500 clients. It did not own up to the attack publicly but did email customers assuring them it was "actively decrypting and restoring data," which implies to us that the ransom was paid.

As of October 2019, 13 managed services providers or cloud-based providers (including TrialWorks) were victims of ransomware attacks causing serious outages to their customers.

There is certainly a lesson here: "This uptick in successful ransomware attacks against MSPs and/or cloud-based service providers is a harsh reminder that organizations have to ensure that the third-party vendors they do business with are as equally protected against the current and emerging cyber threats as they are," said Chris Hinkley, head of Armor's Threat Resistance Unit research team, when he spoke to SC Magazine. "This is especially true because, as we have seen, a successful ransomware attack against an MSP/cloud-based service provider can be debilitating to their customers, as well as to their own company, as the attack can quickly shut down key systems which the customers depend on to run their organization." Yet another reason to check your cyber insurance for coverage of third-party providers.

"And of course, a ransomware attack against an MSP can be fatal, putting an MSP out of business," Hinkley added. He was referencing PM Consultants, an IT consulting firm and support provider for dental practices. The firm shut down in July 2018 after being devastated by ransomware.

So Where Are We Now with Ransomware?

"Ransomware attacks are now data breaches," Abrams said. "During ransomware attacks, some threat actors have told companies that they are familiar with internal company secrets after reading the company's files. Even though this should be considered a data breach, many ransomware victims simply swept it under the rug in the hopes that nobody would ever find out. Now that ransomware operators are releasing victims' data, this will need to change and companies will have to treat these attacks like data breaches."

In case law firms need more bad news, cybercriminals responsible for managing the "Sodinokibi/rEvil" ransomware have indicated that they will follow Maze's course of actions.

This is dreadful news for entities that are very likely facing major fines and other penalties both because they didn't report data breaches and didn't appropriately safeguard customer data. Though most lawyers don't know it, health-care providers must report successful ransomware attacks to the U.S. Department of Health and Human Services.

Final Thoughts

To be frank, the ransomware incidents we've seen previously gave no clue that data had been taken before being encrypted. It is impossible to know how often this was done in the past. Some folks have said publicly that it was an open secret (but we never heard it!). If this tactic becomes the norm, then Abrams is right—ransomware attacks may need to be treated as data breaches and reported. Digital forensics teams may need to be deployed to determine if data was exfiltrated before it was encrypted.

This is a serious game-changer. We have already revised/updated almost all of our cybersecurity PowerPoints!

As we were about to finish editing this column, Reuters reported that cyber insurance companies are increasing their cyber insurance rates by as much as 25 percent—a very large hike! It also reported that the average ransom requested to decrypt files tripled from the first quarter of 2019 to the third quarter. The average ransom was a hefty $41,198 and it doubled again in the fourth quarter to $84,116, a sticker price far beyond the reach of solo and small law firms!

If your law firm hasn't given serious thought to how it will handle a ransomware infection in the future or how it should adjust its incident response plan and its BYOD (bring your own device) policy (we told you in previously columns that acronym really meant "bring your own disaster"), time to roll up your sleeves and get to work.

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* *snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional, Certified Ethical Hacker and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.* *jsimek@senseient.com*.