Small and Midsized Law Firms Slammed by Ransomware

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

A Warning for Law Firms

The first of the quarterly 2021 surveys appeared during April – and the news isn't good for small and midsized law firms. Note these ominous words from Coveware, a highly regarded aggregator of global ransomware and cyber extortion data, which published the Coveware Quarterly Ransomware Report (Q1 2021):

"*The most notable change in industries impacted by ransomware attacks in Q1 was the Professional Services industry, specifically law firms. Small and medium sized law firms continue to succumb to encryption ransomware and data exfiltration extortion attacks. Unfortunately, the economics of many small professional service firms do not encourage or enable adequate cyber security*."

Sobering Statistics from the First Quarter of 2021

The average ransom payment was $220,298 (+43% from Q4 2020)

The median ransom payment was $78,398 (+59% from Q4 2020)

The average number of downtime days was 23 (+10 from Q4 2020)

77% of ransomware attacks include a threat to leak the stolen data (up from 70% in Q4 2020).

Most ransomware-as-a-service (RaaS) affiliates now purchase network access (often for a nominal sum) from someone else, then use the data they can now steal to leverage payment from the victim.

And a new and disturbing trend in 2021? Attackers are taking to disrupting business after an initial attack while the firm is trying to recover – and stealing more data or relaunching ransomware.

What Law Firms Should Assume

Ransomware is no game, but if it were, boy have the rules changed.

The first thing a law firm should assume is that any of its data stolen by attackers will not be destroyed by the cyber criminals even if a ransom is paid. It may well be traded to others, sold – or even held for a second extortion attempt. Those re-extortion attempts are becoming a growing phenomenon.

Also assume that multiple parties held your data and that the data was not necessarily secured and may have been compromised. Also, any of those parties may have made copies for prospective extortion in the future.

It is increasingly likely that data will be published, often called "naming and shaming," before you can even respond to the ransom demand. This ups the ante and puts pressure on the law firm to pay.

Where Does the Danger Come From?

The most common ransomware attack vector is compromised remote desktop protocols, which so many lawyers working from home use to connect to the law firm network.

This is followed by phishing emails, which continue to get better and better at fooling your employees. Employee security awareness training should take place at least annually (more often is better) and running phishing simulations periodically is a good idea. Employees simply forget over time so repetitive training is critical.

Why are Small and Midsize Law Firms So Vulnerable?

As the Coveware report notes, 24.9% of ransomware attacks target professional services firms, especially small and midsize law firms.

So, what are the firms doing wrong? In part, they are hobbled by the modesty of their budgets for cybersecurity. On the other side of the coin, they generally want to maximize profits and distribute income to the partners at the end of the year. Cybersecurity doesn't make the cut when distributions are discussed.

Their clients tend to be smaller and may not demand security assessments as larger clients are prone to do. Sometimes they get to bask in obscurity because attacks on smaller firms often do not make the headlines.

Smaller firms get in a world of trouble because most of them do not have Incident Response Plans (IRPs) and therefore they have a "headless chicken" response to attacks, which they generally don't properly handle. To make matters worse, they don't properly attend to remediation of the vulnerabilities that caused the attack. And you know what happens then? They get re-attacked.

An example of sheer stupidity from our case files. A firm had an Incident Response Plan (IRP). Good for them, right? Except they didn't print it out or put it on a device never connected to the network. So, their IRP was encrypted in the ransomware attack. Doh.

Don't Think Paying the Ransom Will Guarantee You Get All Your Data Back!

Sophos, a highly regarded cybersecurity vendor, issued its "The State of Ransomware in 2021" report. Scary stuff. Their survey found that only 8% of entities get back ALL of their data after paying the ransom. 29% of those who paid the ransom got back no more than half their data. Not only is there no honor among thieves, but there are no refunds for partial performance! In addition, there is no customer service department where you can file a complaint.

There was some good news in the report – sort of. There was a decline of entities hit by ransomware from 51% in 2020 to 37% in 2021. On the face of it, that's a good thing.

But the report notes a very worrisome trend. Attackers are now moving from automated attacks to highly targeted "hands-on-keyboard" hacking. Why is this causing such alarm? Because the potential damage is much greater from these more complex attacks, with more than double the remediation costs, from approximately $761,00 in 2020 to $1.85 million in 2021.

Oh, and to add to the merriment, remediation costs are now ten times greater than the average ransom payment.

Final Thoughts

Not much joy in this article, to be sure. One of the things it proves definitively is that the threats from attackers are morphing constantly. As the threats evolve, so must the defenses. Busy attorneys

understandably have trouble keeping up with cybersecurity. But when they can, they should try to stay current through reading reputable blogs and articles online and taking cybersecurity CLEs at least once a year – and more is better. Batten down the hatches – we're in for a bumpy ride for years to come.

Sharon D. Nelson, Esq. 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