Have Cyber Insurance? The Preferred Victims of Ransomware Attackers

By Michael C. Maschke, Sharon D. Nelson, Esq. and John W. Simek

Like most professional service firms, law firms continue to experience increased cybersecurity attacks, mostly phishing and Business Email Compromise (BEC) attacks, aimed at compromising and stealing payment information. Ransomware attackers, not to be left out, increasingly use phishing attacks as their primary attack vector and frequently target businesses with a cyber insurance policy. Why is that??

Typically, businesses with cyber insurance coverage must have a baseline of cybersecurity measures that insurance carriers require before offering coverage. These measures range from installing Endpoint Detection and Response (EDR) software on all endpoints to requiring staff members to attend annual cybersecurity awareness training.

The cybersecurity measures that may be required vary from carrier to carrier but aim to help reduce the risk of a potential compromise or cyber incident to the insured. Cyber insurance coverage is considered a must-have for law firms of all sizes because of the significant costs associated with investigating and responding to a breach, not including any post-breach expenses related to the notification process of those whose data had been breached and outside counsel costs.

Ransomware attackers are now specifically focusing on targeting businesses with cyber insurance coverage, demanding **more** if their victims have insurance coverage. Research has shown that one of the first steps threat actors take upon compromising a system is to search for documents of a cyber insurance policy.

If evidence of coverage is found, the requested ransom increases on average by a factor of 2.8x, or significantly higher, if attackers can steal sensitive data too. Over the years, ransomware attack victims with cyber insurance coverage pay a ransom almost 50% of the time, compared to around 25% for businesses without cyber insurance coverage.

So, what can you take away from this data? Your firm is being targeted because you have cyber insurance and are historically more likely to pay if you become a victim of a ransomware attack. These are not your average dumb criminals -they will continue to go where the money is.

How can you mitigate your firm's risk of having to pay a ransom? Of course, not getting hit with ransomware in the first place is preferred, but it is not always how things play out. The solution is not solely EDR software, staff training, or having next-gen antivirus installed on

all endpoints *(this helps and is recommended to prevent ransomware)*. The answer is implementing a backup solution immune to ransomware attacks. Having off-site, encrypted, immutable backups in the cloud can ensure your business continuity and eliminate the need to negotiate with ransomware attackers to lower your ransom.

Ransomware outbreaks typically encrypt your local computer hard drive, network file shares from servers, and any directly connected USB device or Network Attached Storage, including external hard drives. Having an immutable backup that cannot be changed or altered, and beyond the reach of ransomware's encryption processes, is the only way to ensure your firm's ability to restore its critical files and client data. Over the last several years, we have seen several law firms go out of business because they did not have a ransomware-proof backup solution and could not afford to pay the ransom.

Of course, it is preferred not to get ransomware in the first place. You can mitigate that risk through some of the common recommendations, including EDR software, encryption, cybersecurity awareness and phishing training, following the security principle of least privilege, limiting usage of Administrator accounts and access, and by following other basic cybersecurity controls. The less you protect, the more in danger your firm will be.

Michael C. Maschke *is the President and Chief Executive Officer of Sensei Enterprises, Inc. Mr. Maschke is an EnCase Certified Examiner (EnCE), a Certified Computer Examiner (CCE #744), an AccessData Certified Examiner (ACE), a Certified Ethical Hacker (CEH), and a Certified Information Systems Security Professional (CISSP). He is a frequent speaker on IT, cybersecurity, and digital forensics, and he has co-authored 14 books published by the American Bar Association. He can be reached at mmaschke@senseient.com.*

Sharon D. Nelson *is the co-founder of and consultant to 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 the co-founder of and consultant to Sensei Enterprises, Inc. He holds multiple technical certifications and is a nationally known digital forensics expert. He is a co-author of 18 books published by the American Bar Association. jsimek@senseient.com*