The Cybersecurity Control Money Can't Buy

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

Law firms spend enormous amounts of money protecting their networks. They use firewalls, endpoint detection, multifactor authentication, security monitoring, and email filtering. The list of technologies designed to keep attackers out keeps growing. And yet, sometimes an attacker doesn't need to defeat any of them.

Recent reports of cyberattacks on some of the world's largest law firms offer a sobering reminder of that reality. WilmerHale reportedly paid at least $18 million to the cyber extortion group Luna Moth after an attack, while Goodwin reportedly paid about $10 million. Weil reportedly paid between $18 million and $20 million after a separate incident. Combined, the ransom payments alone approach $50 million.

Those figures are staggering, but the ransom amounts aren't the most important part of the story.

The Attack Wasn't Necessarily Sophisticated

Goodwin said its incident began when a single employee was deceived into providing credentials to an unauthorized person. In another recent incident, Mayer Brown said an employee mistakenly sent documents to someone who had misrepresented their identity. The firm said the third party never gained access to its systems.

Different incidents, but each has the same underlying lesson. Sometimes the easiest way to bypass sophisticated cybersecurity defenses is to simply convince someone to help you.

Social engineering has existed for decades, but attackers continue to refine it. Today's attacks may involve someone impersonating an IT technician, calling an employee directly to request remote access, or creating enough urgency and credibility that the victim believes the request is legitimate.

That poses a particularly difficult challenge for law firms because attorneys and staff are trained to be responsive. Clients expect quick answers, and partners want problems solved. Attackers understand these workplace dynamics and exploit them to their advantage.

Technology Can't Fix Everything

None of this means firms should stop investing in cybersecurity technology. Strong technical controls remain essential and can limit damage even after a mistake occurs. But technology has limits.

An employee who voluntarily provides credentials may circumvent protections designed to prevent unauthorized access. Someone who approves a multifactor authentication request they didn't initiate can defeat one of the industry's most important security controls. An employee who grants remote access to someone they believe is from IT may effectively escort an attacker past a layer of expensive security technology.

That's why cybersecurity awareness training can't be an annual video employees click through while answering email. Employees need to understand how attacks happen and how to independently verify whether someone claiming to be from their IT department or technology provider is legitimate. Most importantly, they need permission to slow things down when something doesn't feel right.

Make Verification Normal

Law firms can make social engineering significantly harder by establishing simple verification procedures.

If someone claiming to be from IT unexpectedly contacts an employee, the employee should know how to verify that person's identity using a trusted phone number, an internal messaging system, or an established help desk process. Requests involving passwords, remote access, financial transactions, sensitive documents, or multifactor authentication should automatically trigger additional scrutiny.

The goal isn't to make employees suspicious of everyone. It's to make verification part of the firm's culture. Attackers thrive on urgency. They want employees to act before thinking, whether the request supposedly comes from the managing partner, the accounting department, an IT provider, or an important client.

A culture that encourages employees to pause and verify unusual requests removes one of the attacker's greatest advantages.

The Human Element Still Matters

Another lesson buried in these enormous ransom figures is that cybersecurity isn't only a problem for firms without adequate resources.

The firms being targeted are among the largest and most sophisticated legal organizations in the world. They have substantial technology budgets, experienced security

professionals, and access to virtually every cybersecurity tool available. Attackers are successfully targeting people all the same.

That's something every law firm should consider, regardless of size. You can spend a fortune making the locks on your doors stronger. But if someone can convince an employee to hand over the key, those locks suddenly matter a lot less. The answer isn't more fear. It's better preparation, better training, and a workplace where verifying an unusual request isn't treated as an inconvenience.

Sometimes the most important cybersecurity question an employee can ask is also the simplest, "How do I know you are who you say you are?"

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.*