When Cyberattacks Walk Through the Front Door

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

For years, law firms have invested heavily in defending against remote cyberattacks. Firewalls, multifactor authentication, endpoint detection, email security, and employee awareness training have become standard components of modern cybersecurity programs. The underlying assumption has been that attackers would try to gain access through the firm's technology infrastructure. Increasingly, however, cybercriminals are succeeding by exploiting something much simpler: human trust.

Recent reporting from Google, Mandiant, and the FBI describes an extortion group that has moved beyond traditional phishing emails and phone scams. When victims refuse to cooperate with fake IT support calls, members of the group have reportedly appeared in person at offices, posing as technicians and attempting to gain physical access to computers via USB devices. While these tactics may sound like something from a Hollywood movie, they reflect a broader shift in how sophisticated threat actors approach their targets. Cybersecurity is no longer confined to the digital world.

Social Engineering Is Evolving

Most law firms have spent years training employees to recognize suspicious emails. Staff members are encouraged to verify unexpected requests, avoid unknown links, and report questionable attachments. Those efforts have paid dividends, making traditional phishing campaigns less effective than they once were.

Rather than abandoning social engineering, many attackers are adapting. Today's scams increasingly start with a convincing phone call, a request for remote support, or a visitor at the reception desk claiming to be from the firm's IT provider. Criminals know that people are often more willing to trust a friendly voice or a professional-looking visitor than an anonymous email. The technology behind these attacks has not changed dramatically, but the methods of deception continue to evolve.

Physical Security and Cybersecurity Are No Longer Separate

This evolution should prompt law firms to rethink how they define cybersecurity. A visitor requesting access to a workstation may represent just as much risk as a phishing email. Receptionists, legal assistants, attorneys, and office managers all contribute to the firm's security posture because they are often the first people an attacker encounters.

That raises practical questions every firm should consider. Would employees know how to verify that an IT technician was properly scheduled to be on-site? Would anyone question an unexpected request to connect a USB device or perform workstation maintenance? Does the firm require outside vendors to check in through a documented process before accessing systems or offices? These may seem like operational details, but they are increasingly part of cybersecurity controls.

Trust Still Needs Verification

One of the more concerning aspects of these attacks is their speed. According to Google's investigation, attackers sometimes moved from initial contact to data theft in less than an hour, with extortion demands following shortly thereafter. That leaves organizations with very little time to recognize what is happening before sensitive information has already been compromised.

Fortunately, the response does not require expensive new technology. The same principles that make organizations resilient to phishing attacks apply here as well. Verify unexpected requests, confirm identities through trusted channels, escort visitors who need access to sensitive areas, and ensure employees understand that questioning unusual activity is encouraged.

Law firms have made tremendous progress in strengthening their technical cybersecurity defenses over the past decade. The next challenge is recognizing that cybercriminals no longer view the physical office and the digital network as separate environments. Neither should we. The next significant cyber incident may not begin with a malicious email or an exploited vulnerability. It may begin with someone walking through the front door, introducing themselves as "IT support," and hoping no one asks any questions.

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.*