Physical Security in a Transformed World

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

The Evolving Practice of Law

It has been several years since we wrote on the topic of physical security, but it seems like a good topic now that so many law firms are changing how lawyers work. While there are some law firms demanding that all their lawyers return to work, more and more law firms have settled into a hybrid workplace environment. Many cybersecurity topics are sexier, but maintaining physical security is more critical now than ever.

Old-fashioned Physical Security

Pre-pandemic, we thought about conventional physical security (which some law firms still do not have). We had self-locking doors, security cameras, alarm systems, locked file cabinets and locked server rooms. We monitored for water leaks, fires, and unauthorized entry into our law firm.

For a long while, physical security didn't seem like a big deal. And then came COVID.

The Impact of the Pandemic

In every cybersecurity webinar we give, we have a "See something? Say something!" slide. But for a very long time, we had a dispersed workforce. At the very beginning of the pandemic, most law firms had a skeleton crew. In smaller firms, sometimes only the office manager came to work every day to answer phones, clear voice messages, pick up mail and deposit checks. As we straggled back to work, many stayed home – and that added to a decline in physical security because there weren't as many eyes on what was happening at the office.

Even that issue was dwarfed by the work-from-home employees, whose networks are 3 ½ times more vulnerable to attack. But to return to physical security, many of those at home had smart devices that might or might not be listening in on confidential calls. We began to see law firms issuing alerts to employees, advising them to turn off smart devices if they were going to engage in a confidential conversation.

Employees were also asked to work in a private room, which was not possible for everyone. Some of those people created an office in a shed, trailer, or other unusual accommodation. There was less physical security with those arrangements. No matter where employees worked from home, computers were not necessarily locked when the employees left the laptop for a few minutes – and files were often left in the open.

Not everyone locks their doors at night (somewhat surprising in these times) and while many have home security systems – including exterior video surveillance – many do not. Many firms haven't asked about any of this.

Attorneys were sometimes (and sometimes not) asked to wear headphones for confidential conversations, making it impossible to hear more than one side of the conversation.

More policies followed, forbidding that a work device be shared with a spouse or children. And while personal devices were used at first, more and more law firms began to deploy firm-owned devices to replace the use of personal devices – and extending the law firm's security technology and policies to those devices.

How Good is Your Physical Security?

COVID threw everyone off the rails, but it is time to return to assessing your law firm's physical security. Many firms never made assessments of home offices. Therefore, many firms will be starting all over again, this time taking the work-from-home folks into account.

Getting a physical security assessment from an expert is the best way to proceed and that should be done right away, especially if attention to physical security lapsed during the pandemic. At this point, many cybersecurity experts have crossed over and including physical security in their overall cybersecurity assessments. For most law firms, especially the smaller ones, it is more economical to have both assessments done by one party – and you can generally get an expert to "flat fee" the pricing so you can budget for the assessment.

One of our friends tested the security of a law firm client by dressing as a janitor and "catching" the locked door to the building as someone went in using their prox card. He was unchallenged and able to enter a law firm and walk around without being questioned. Two major lessons there – don't defeat your security by allowing others to "use your credentials" to get in – and be watchful for people you do not know roaming the office.

Famously, some years ago, a woman got in a law firm in much the same way described above. She walked around the law firm without being questioned. She even (unbelievably) sat in on a meeting in the law firm's conference room. No one asked her who she was. After the meeting, she wandered around the law office stealing money from purses and smartphones. Yes, she was finally caught (she'd done similar things many times) and went to prison, but she remains one of our favorite stories emphasizing the critical nature of law firm physical security!

Final words – Why We Love Our Panic Buttons

No physical security system will be perfect. But you should be able to greatly reduce your risk. Policies, technologies and oversight by your employees are all part of the mix.

Highly recommended are emergency panic buttons that silently send an alarm to your local police department. You do have an alarm system, don't you? Like so many other people, we have had a potentially dangerous, very drunk and threatening individual show up in our office.

Panic buttons are much more widely in place now in law firms. May you never need to use one, but they certainly can "save the day."

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 (CISSP), Certified Ethical Hacker (CEH) 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*.

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.* *mmaschke@senseient.com*.