Law firms are tempting targets for hackers. Firms, clients, peers, and various third parties exchange massive amounts of data in multiple unsecured formats and mediums, many of which have no guarantee of cleanliness. Law firms also advertise high-profile cases and clients on their websites. These cases are in the news and on court calendars. Lawyers often work long hours, and they often want or need access from both personal and business-allocated assets from a variety of locations. Unfortunately, many attorneys do not “get” technology or cybersecurity. Law firms are notorious for not spending enough money on security or a hardened technology infrastructure.

Given all the juicy incentives and vulnerabilities present in most law firms, it is no wonder hackers target them. However, the vast majority of firms and companies are hacked using simple techniques such as social engineering. Some common sense and cost-effective practices can reduce vulnerabilities from these, and other, more sophisticated attacks. Even the smallest firms can afford to protect themselves.

Take for instance this scenario, based on a true story, describing how most organizations get breached. Names and specific circumstances have been changed.

Josh is a partner at a national law firm. The information contained in many of the matters Josh manages is lucrative to hackers. Josh’s firm was handling a financial fraud case that could land many well-known people in jail. The information from this matter was very appealing to both independent hackers and those for hire by interested parties, resulting in Josh’s firm being targeted for Advanced Persistent Threat (APT). An APT usually means the hackers will attempt to gain access but remain low-key to avoid detection. They will slowly and consistently harvest information and use the law firm to gain further access to clients and other law firms.

The hackers first performed reconnaissance on employees of the law firm. They knew social characteristics that they could target from the employee’s online activity: likes, dislikes, social media groups, events attended, and friends. There were many targets, but they only needed one to take the bait. The hackers found that Josh’s paralegal, Channing, was a huge fan of the band Maroon 5 and had been searching the web and asking people online how she could get tickets to an upcoming concert. Channing had also subscribed to a popular radio station newsletter for chances to win tickets.

The hackers sent the paralegal a fake email that appeared to be from a local radio station announcing a free ticket raffle for the upcoming Maroon 5 concert. The email contained a link to a registration website. Once Channing clicked on the link, a zero-day browser exploit was executed. These are usually undetectable by anti-virus and host-based prevention systems. The exploit also opened up a port from which the hacker accessed Channing’s machine, where they set up a reverse Transmission Control Protocol (TCP) connection on the server in order to gain access to the network. Once on her machine, they immediately started pulling files from the file servers and document management systems.

A week later, critical files and email contents were posted to some underground websites where they were sold to the highest bidder.
Finally, the third party should conduct a test to ensure response readiness when a data breach or cyberattack occurs.

Know yourself:
When security firms perform scans on their law firm clients, they find software, data transfers, processes, and devices that the law firm did not know existed. In lieu of deleting or removing these items, law firms often choose to let software, services, and firewall rules remain because they do not know who may need them. Hackers can hide their activities in the noise of your network and the unknown attached devices. They depend on the victim not knowing the difference between normal and anomalous behavior. Know and document connected devices to your network, and note changes to your environment. Do this as well for business-critical information, software, and services. Most systems have settings to disallow unauthorized software to run on your machines, just as there are alerts and embedded settings that tell you when changes occur. The better the firm knows itself and controls the resources it has, the better it can detect anomalies in its systems. This does not require you to become a technology expert; it just requires that you be more vigilant about knowing what is in your IT environment.

How could Josh’s law firm have prevented or detected a hack such as this? Let’s start with the basics. The following are what security firms call Foundational Cyber Hygiene (FCH) or Foundation Security Controls (FSCs) that focus on preventing an attack or detecting and remediating when an attack occurs.

01 Separate work and personal online activities: Personal activities such as shopping, searching for concert tickets, or using personal social media sites should not be performed with a work email account or via a work internet connection. Do not reuse user IDs and passwords for both work and personal activities. If Channing had not been using her work email address to look for tickets, an email from the radio station would have been immediately suspicious. In addition, the use of her work email address allowed for more advanced reconnaissance scanning that revealed information about her firm.

02 Regular cybersecurity training and testing for employees: Training, and testing the efficacy of the training, is critical. Effective training should not use scare tactics, nor should it attempt to train employees to be technology or security experts. Effective training and testing uses common-sense practices and tests against those practices. Identifying social engineering techniques should be a part of any cybersecurity training. Employees should also be able to detect a suspected cyberattack and/or breach.

03 Define security policies and procedures: Employees do not always understand why security policies and procedures are put into place. This causes people to find ways to work around them or not follow them because they consider such policies an impediment to productivity. Security policies need to be defined in language that is easy to understand. Provide examples that put the policies into context. “Bring Your Own Device” (BYOD) policies are particularly critical.

04 Use credentialed third-party security providers for support, monitoring, testing, and validation: The core competency of a law firm is to practice law, which means that managing a technology staff is usually a low priority. Therefore, it is highly recommended that law firms hire a cybersecurity firm to perform vulnerability and cyberbreach response testing on a periodic basis. These tests will indicate if software and hardware have been patched, if the rules on your firewalls are up to date, if your websites are vulnerable to a hacker trying to impersonate, deface, or get to your client information, and much more. Monitoring includes a review of possible exfiltration of data.

Finally, the third party should conduct a test to ensure response readiness when a data breach or cyberattack occurs.

05 Know yourself: When security firms perform scans on their law firm clients, they find software, data transfers, processes, and devices that the law firm did not know existed. In lieu of deleting or removing these items, law firms often choose to let software, services, and firewall rules remain because they do not know who may need them. Hackers can hide their activities in the noise of your network and the unknown attached devices. They depend on the victim not knowing the difference between normal and anomalous behavior. Know and document connected devices to your network, and note changes to your environment. Do this as well for business-critical information, software, and services. Most systems have settings to disallow unauthorized software to run on your machines, just as there are alerts and embedded settings that tell you when changes occur. The better the firm knows itself and controls the resources it has, the better it can detect anomalies in its systems. This does not require you to become a technology expert; it just requires that you be more vigilant about knowing what is in your IT environment.
06 **Control use of administrative privileges:** Obtaining user credentials, particularly when that user has administrative-level access to devices or services, is the golden ticket for hackers. A user on a network must have workstation administration or domain administration rights to install software or any other executable file on a networked-attached machine. Administrators have the ability to create other users with access rights on the network; sometimes those other users are other administrators. In order to control a firm’s environment, a malicious attacker will obtain user access rights and then “elevate” those privileges to gain administrator rights. It is similar to a criminal getting a copy of a spare key to your house, but you were unaware because you had not kept track of how many spare keys you have. Take inventory of administrator privileges and validate them frequently.

07 **Use strong passwords and multi-factor authentication:** As stated in the previous section, hackers want credentials. Using multi-factor authentication, when available, makes getting access to credentials difficult. Implementing this involves adding another layer of security to your password such as a fingerprint, a cell phone code, an emailed code, or a combination of all of those methods. The second way to makes accessing credentials difficult is to have a “strong” password and a unique user ID. A strong password has a minimum of 12 characters and uses a variety of case and special characters. To help remember a password, many people use the first or last letter of a song title, a long sentence, a theme, etc. An example is:

- The Sound of Music with Julie Andrews won 5 academy awards and was nominated for many more = TSOMwJAw5aawfnmm
- An even stronger version would be replacing or adding special characters: TSOMwJAw5a@awfnmm8

08 **Change your passwords, but not as often as you might think:** People complain about having so many passwords to remember. Often, when people are forced to change their passwords every 90 days, they use simpler passwords or make predictable changes to them. People also tend to leave password change requests and temporary passwords in their email accounts. Always change your password if you have reason to believe it has been stolen or compromised, and never leave the default username or password on any login. At a minimum, change your password at least once a year, but not every 90 days. When you do change your password, make sure it is not related to the old one, and do not reuse one from another account. There are settings on most network domains and in Active Directory (AD) that note frequency, password history, strength, and similarities to previous passwords in order to enforce password best practices.

09 **Never log into an open Wi-Fi or Bluetooth connection without added security:** A packet analyzer, also known as a “sniffer,” can detect information sent over an unsecured network. Never log into an open, free Wi-Fi site (like at your local coffee shop) without encryption, and ensure your websites have some level of encryption, like HTTPs, Secure Sockets Layer (SSL), or Virtual Private Network (VPN). If you or your firm does not have a VPN, get one. Many systems and network appliances have one built in. Also, for those who log into password-protected Wi-Fi networks, keep in mind that if the network password is known to the attacker, they will be still be able to snoop on the data or packets traveling over the network.

10 **Above all, use common sense:** Despite the terms and complexities of security in cyberspace, it is not that much different from the physical space.

Studies show that organizations with a handle on the Foundational Cyber Hygiene (FCH) and related controls are roughly 90 percent less likely to suffer a breach. However, implementing FCH is not a one-time event and it is not a magic pill. Changing technologies, vulnerabilities, attack vectors, and methods appear all the time. Therefore, performing these measures, keeping your staff trained and informed about security controls and practices, using specialist firms to help you understand your vulnerabilities, and monitoring for any unusual practices will reduce your chances of being attacked. Your firm will also more easily detect an attack should one occur.

---

**Mary Frantz**

maryf@ekpartner.com

Ms. Frantz is the CEO and managing partner of Enterprise Knowledge Partners (EKP), a national firm with headquarters in Bloomington. EKP specializes in technology, forensics, e-discovery and cybersecurity. She has over 25 years’ experience and holds six degrees, as well as certifications in multiple practice areas.