The First Step Toward Protecting Your Firm

Hackers and Why They Hack—and Why You Need to Know

By Darius K. Davenport and W. Ryan Snow

Lawyers must understand the threats before they can build a comprehensive cybersecurity plan—one that addresses IT security, incident response, cyber-employee policies, and cyber insurance coverage.

The terms "cybersecurity" and "hacking" have become ubiquitous. Every few weeks, we hear of another major business that became the latest victim of a hacker. In 2014, hackers were rumored to have taken more than 100 terabytes of data during the Sony breach. James Cook, *Sony Hackers Have Over 100 Terabytes of Documents. Only Released 200 Gigabytes So Far*, Business Insider (Dec. 16, 2014). In 2015, hackers compromised the personal information of 191 million registered voters. Nate Lord, *The Top 10 Biggest Data Breaches of 2015*, Digital Guardian (July 27, 2017). In 2017, Yahoo confirmed that hackers compromised usernames, email addresses, telephone numbers, security answers, dates of birth, and hashed passwords (passwords that have been mathematically converted into a random-looking string of characters to prevent them from being misused) for all 3 billion of its user accounts. Robert McMillan & Ryan Knutson, *Yahoo Triples Estimate of Breached Accounts to 3 Billion*, Wall St. J. (Oct. 3, 2017).

Law firms have not been immune. To name a few, in 2016, hackers attacked large firms such as Cravath, Weil, and Mossack Fonseca (which later failed). In 2017, hackers attacked DLA Piper. Countless small and medium-sized firms have become victims as well. Nearly 40 percent of 200 firms surveyed by LogicForce had been hacked and didn't even know it. *See Ian Lopez, DLA Piper Isn't Alone—40 percent of Law Firms Unaware of Breaches,* Law Journal Newsletters (Aug. 2017).

So who are these mysterious hackers? Why do they hack, and why do they care about lawyers, especially small and medium-sized firms? Understanding hackers and the cybersecurity risks that they pose is the first step toward protecting your law firm.

■ Darius K. Davenport leads the Cybersecurity and Data Privacy Practice Group of Crenshaw Ware & Martin in Norfolk, Virginia. His practice focuses on data privacy laws and regulations, helping clients mitigate cyber risk, and dealing with the legal and practical problems resulting from cyber incidents. His cybersecurity counsel to businesses and municipalities includes drafting and review of incident response plans, cybersecurity employee policies, technology contracts and conducting cybersecurity and breach response exercises. W. Ryan Snow is managing partner of Crenshaw Ware & Martin. He handles complex business disputes, with a focus on government contracts, cybersecurity, construction law, and maritime law. He also serves as local counsel in the Eastern District of Virginia in patent and other intellectual property cases.

Who Are the Hackers?

The true definition of a "hacker" is an expert at programming and solving problems with a computer. *Merriam Webster*. However, we have come to know hackers as individuals who illegally gain access to and sometimes steal or tamper with information in a computer system. *Id.* Hackers are far from a monolithic group of individuals that lurk in the "dark web" to steal data. There is not enough time or space here to discuss the details of every kind of hacker. The following kinds of hackers, however, are most relevant to attorneys and their clients.

- **Advanced Persistent Threats (APTs):** According to Secure Works, an APT is a highly sophisticated, stealthy continuous computer hacking group that usually targets private organizations, states, or both, for business or political reasons. *Advanced Persistent Threats: Learn the ABCs of APTs - Part A*, Secureworks (Sept. 27, 2016). Advanced persistent threats are known to burrow deep into target networks to avoid detection, sometimes for years. *Id*. The stealth nature of their sophisticated operations allows them not only to evade detection but to extract significant amounts of data from victims. *Id*. They are usually associated with nation states, cyber espionage, or sophisticated organized crime organizations. It is believed that a nation state, deeply entrenched in Sony's computer system for a long period of time, was responsible for the massive hack of 2014. *See* James Cook, *Sony Hackers Have Over 100 Terabytes of Documents. Only Released 200 Gigabytes So Far*, Business Insider (Dec. 16, 2014). Individual hackers usually lack the resources or sophistication to act as an APT.
- **Crime Organizations and Industrial Spies:** The next hackers are organized crime groups and industrial spies. These hackers are motivated by money. *See* Roger A. Grimes, *IT's 9 Biggest Security Threats*, CSO (Aug. 10, 2017). They use high-end social engineering, spam, phishing, and spyware or malware to commit identity theft and fraud or to gain unauthorized access to an organization's systems. *Id*. Industrial spies and organized crime groups are also sophisticated. They can rival APTs or even be associated with APTs. Organized crime groups and industrial spies usually target organizations, because they are in search of trade secrets, market information and intellectual property, or they are simply seeking to damage a competitor's reputation by attacking an IT infrastructure. *Id*.
- **Unorganized Criminals:** The third kind of hacker is the unorganized criminal. These hackers can be individual hackers or smaller, less-sophisticated groups of hackers. Unlike APTs, organized crime organizations and industrial spies, the unorganized criminals' skill level can vary dramatically, from attackers who are able to write and propagate malicious code to those who simply purchase and deploy malware obtained from the dark web. *See* Grayhat4Life, *7 Types of Hackers You Should Know* (Sept. 9, 2015). Most are motivated by money, while others are motivated by the notoriety associated with penetrating well-known IT systems.
- **Hacktivists:** The last kind of hacker is the hacktivist. Hacktivists' goals are typically associated with supporting a political agenda. *See* Jenni Bergal, "Hacktivist Launch More Cyberattacks Against Local, State Governments," *PBS News Hour*, Jan. 10, 2017. Their subgoals are propaganda and causing damage to achieve notoriety for their cause. *Id*. Hacktivists may be less of a concern for lawyers, but more of a concern for a lawyer's clients.

Advanced persistent threats, organized crime groups, industrial spies, criminal hackers, and hacktivists are all different groups with different motivations for why they hack. But the majority of hackers are motivated by one thing: money.

Why and How Hackers Hack

The primary motivation for hackers is money. Since the early 2000s, hackers have developed an underground economy to monetize stolen data. The method used to monetize hacking is closely related to the attack vector used. The three major attack vectors for monetizing data are

- selling the stolen data on the black market;
- holding data for ransom and profiting from payments made to release the data; and
- intercepting or initiating a wire transfer.

The Black Market for Stolen Data

McAfee's "The Hidden Data Economy Report" describes stolen data as the "oil of the digital economy." Data is one of the fastest-selling commodities on the dark web. Richard, *The Value of Stolen Data on the Dark Web*, DarkWebNews (July 1, 2017). Underground markets on the dark web sell stolen data that consists of everything from hotel loyalty accounts and online video streaming credentials, such as Marriot Rewards or Netflix, to financial institution log-in credentials and health-care records. *Id.* Cybercriminals can sell data in bulk for as little as $0.50 a file for entertainment credentials or up to $200 a file for bank credentials. Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Apr. 9, 2018). Health-care files are considered a hacker gold mine because of the vast amount of personal information that they contain. *Id.* On average, individual medical records retailed between $70 and $100 last year. *Id.* Similar to any other marketplace, the price per file fluctuates based on the supply and demand for a particular type of data file. *Id.*

Hacktivists may be less of a concern for lawyers, but more of a concern for a lawyer's clients.

Ransomware Attacks

One major way that hackers monetize stolen data is through ransomware attacks. The public's familiarity with the term ransomware grew exponentially after the 2017 WannaCry ransomware attack. Generally speaking, ransomware is a form of malicious software (or malware) that takes over a computer and can either deny its owner access to data, delete data, or threaten to delete data. Josh Fruhlinger, *What Is Ransomware? How It Works and How to Remove It*, CSO (Nov. 13, 2017). After the attack is triggered, the attacker contacts the victim promising to restore the victim's access in exchange for payment of the ran-

som. *Id.* The cost of a ransom can range from a few hundred dollars to several hundred thousand dollars, generally payable in some form of cryptocurrency, such as bitcoin. *See* How to Protect Networks from Ransomware, FBI (ransomware prevention and response for CISOs, U.S. government interagency technical guidance). But it is not guaranteed that a victim's data will be restored after payment is made. *Id.* That is why law enforcement recommends not paying the ransom, because payments only encourage the cybercriminals' enterprise. *Id.* Instead, organizations should maintain consistent backups of their data. *Id.* Well-prepared organizations should also have thoughtful incident response plans that are prepared by outside breach counsel.

In addition to personal information and health records, firms are also rich sources of trade secrets and intellectual property.

Malicious ransomware software is usually delivered as the result of a phishing email campaign during which an unsuspecting victim is tricked into clicking on a malicious link or attachment masquerading as a legitimate file. *Id.* Once the file is opened, the malware takes over the victim's computer. *Id.* Some more aggressive variations, such as NotPetya, exploit security holes in software to infect victim's computers without the use of social engineering trickery. Timothy B. Lee, *The WannaCry Ransomware Attack Was Temporarily Halted. But It's Not Over Yet*, Vox (May 15, 2017.)

Business Email Compromise

The third popular attack vector for hackers is an emerging financial cyber threat called "business email compromise" (BEC). FBI, *Business E-Mail Compromise*, News (Feb. 27, 2017). The FBI started tracking this vector in 2013.

Business email compromise works by hackers targeting employees with access to company finances and then tricking them into making wire transfers to bank accounts controlled by the hackers instead of the bank accounts of legitimate business partners. *Id.*

Hackers use spear phishing, social engineering, identity theft, email spoofing, and malware to gain access to their victim's computers. *Id.* They may spend weeks or months modifying a victim's email rules and settings; studying the organization's vendors, billing systems and transactions; and studying the victim's communication style and personal calendar. *Id.* Hackers then discreetly hijack legitimate communications and request that legitimate payments be sent to fraudulent accounts. *Id.* The perpetrators are so skilled in the deception that the fraudulent wire transfers are often not detected until too late. *Id.* Hackers have targeted every business sector to include law firms. The FBI estimates BEC losses to be in the billions. *Id.*

Why Law Firms Are Targets

There are three major reasons why law firms are targets: (1) all data, including law firm data, has black market value, and law firms often hold valuable confidential information; (2) hackers don't discriminate when it comes to victims; and (3) law firms are soft targets.

Data Has Black Market Value

As discussed above, hackers (no matter what skill level), have found a way to monetize stolen data. This can include a firm's entire IT infrastructure in the case of a ransomware attack. For lawyers, that means that insufficiently protected employee and client information (both of which attorneys have a duty to protect) is a cash crop ripe for hackers to harvest and sell.

Large caches of medical records make a law firm a prime target for hackers. Health records contain names, addresses, phone numbers, account numbers and the names of family members that are often used in passwords or as account security questions. Many firms store this kind of personal health information (PHI) in their computer systems. This naturally makes law firms a rich source of PHI data to be traded on the black market.

In addition to personal information and health records, firms are also rich sources of trade secrets and intellectual property. Clients provide firms with intimate details of their businesses and products during the course of representation. Similar to PHI, trade secrets and intellectual property are stored on firm computer systems, making them ripe for theft or ransom.

In addition to data theft, law firms are businesses, and just as any other business, a law firm's IT infrastructure can be subject to ransomware attacks. During one of these attacks, a hacker can lock up and encrypt client data, payroll, communications, and other office systems for ransom—effectively shuttering those assets. The result is that the firm's ability to serve its clients will be severely hampered until the systems are restored. These attacks can be uniquely damaging because, even if office functions can be quickly restored, firm data may never be recovered. For example, after a severe ransomware attack, one firm lost over a decade's worth of internally developed programs and databases that the firm will never be able to recreate.

A recent ransomware example is the DLA Piper hack of 2017. The breach took the firm's computer and phone systems off-line in offices in the United States, Europe, and the Middle East. Alex Aldridge, *DLA Piper Rocked by Ransomware Attack… Weeks After Publishing 'How to Protect Against Cyber Attacks' Guide*, Legal Cheek (Jun. 27, 2017). Although not all computer systems were affected, it was necessary to take all of them off-line to contain the attack. James Booth, *DLA Piper Hack Could Cost 'Millions', Brokers Say*, Legal Week (July 7, 2017). The hackers requested 300 bitcoin (U.S. $2,579,998) in ransom to release the firm's data. Jonathan Crowe, *How One of the World's Largest Law Firms Was Paralyzed by Petya*, Barkly: Blog (July 2017). DLA Piper did not pay the ransom. *Id.* Even though the firm did not pay, cyber insurance brokers estimate that it will cost millions to remediate the effects of the hack. *Id.* In addition to the cost of remediation, Roy Strom, from The AmLaw Daily, observed that thousands of billable hours were lost as a result of "litigators unable to access motions on a deadline, trial lawyers preparing for arguments without key documents, and transactional lawyers unable to communicate with clients attempting to close multibillion-dollar deals." *Id.*

Hackers Don't Discriminate When It Comes to Victims

When it comes to victims, hackers don't discriminate. It does not matter whether a firm is big or small. It doesn't matter if a firm perceives its data to be of high value or little value to hackers. The reality is that if a firm uses computers, (1) its data can be stolen, (2) its systems can be held for ransom, and (3) its wire transfers can intercepted. According to the 2017 Verizon Data Breach Investigation Report, hackers attack all sizes of organizations. *2017 Data Breach Investigations Report*, Verizon (2017). Hackers also attack all industries, including the public sector, manufacturing, retail, education, finance, utilities, health care, and of course the service industry, which includes law firms. *Id.*

Firms Are Soft Targets

Unfortunately, most law firms are uniquely soft targets, typically more so than their clients. Many business clients have taken significant measures to harden their IT infrastructures to protect trade secrets or intellectual property. Those same clients then take that information to their attorneys, who usually have not applied the same measures to protect their own IT infrastructure. Hackers know this. That's why they seek out a company's law firm instead of the company itself.

Law firms are also attractive targets for hackers because a single firm can give a hacker access to sensitive information for multiple high-profile clients. Ian Lopez, *China Hacks on US Corporations Rising, With Law Firms and GCs Prime Targets*, The Am. Lawyer Int'l, Law.com (Apr. 13, 2018). General counsels in private firms are among the top targets for sensitive information because they have access to much of the same information as the CEO, but they don't have the same level of security. *Id.* Hackers can attack one soft target and gain access to the data of multiple clients in one fatal hack. This makes attorneys very attractive targets. It also should encourage lawyers to take the threat of cybersecurity more seriously and realize that it is not just an IT issue.

Conclusion

Hackers are a diverse group. Yet despite their diversity, the majority of them are driven by the same thing: money. Hackers have essentially monetized data, and lawyers (no matter the practice area) have a lot of data that a hacker can turn into profit. In today's technology-fueled world, lawyers need to understand that they can't continue to ignore cybersecurity. Forward-thinking lawyers must understand the cyber threat—both to their law firms and their clients—and build a comprehensive cybersecurity plan to address IT security, incident response, cyber-employee policies, and cyber insurance coverage. FD