in practice

Cybersecurity: You Can't Afford to Ignore It Anymore

J. Randolph Evans and Shari L. Klevens

April 25, 2016

In late March, newspapers confirmed that a Russian hacker named "Oleras" targeted 48 law firms (most of which are Am Law 100 firms). Oleras planned to hack these firms to secure confidential and highly valuable insider information regarding mergers and acquisitions that the hacker could then use on the market.

In the wake of the recent attacks on the group of elite law firms, the Department of Justice is investigating whether any confidential information was stolen, and for what purpose. Separately, a plaintiffs' law firm has also announced its intent to bring a class action legal malpractice lawsuit against firms for failing to properly protect client information from hackers. But this is just the beginning.

Now, reports center on a growing scandal arising out of the "Panama Papers"—confidential files held by a Panamanian law firm consisting of legal records and documents for law firm clients engaged in secret banking and tax matters in Panama. The law firm was hacked. The leaked papers have drawn attention to the activities of the law firm and their clients, including investigations into whether their conduct was proper.

A firm trading in the ability to protect the confidentiality of their clients' activities was suddenly exposed—both figuratively and literally. From the seemingly manageable challenges of lost laptops and unsecured networks to the real-life confirmation of targeting of firms by international computer hackers, cybersecurity is an issue that can be ignored no longer. It is a risk that grows every day.

Technological terrorists using sophisticated computer skills including hacking and spying are focusing on law firms more than ever. One recent scam, targeting 100 companies (approximately 20 percent of which were law firms), launched phishing attacks that secured passwords, penetrated superficial firewalls, and gained access to extremely sensitive information.

Gone are the days when attorneys could easily identify an email scam written in broken English and using suspicious wording. Current phishing scams say the right things and use the right terminology. And, increasingly, they utilize confidential data in the newest form of corporate
extortion.

For attorneys and law firms, the risks are much more than financial. Bar rules obligate attorneys to protect client information, with potential discipline lurking in addition to whatever financial damage a client may suffer.

The level of risk has increased to such an extent that even government agencies—including the Department of Defense—can be fooled. An errant click or a simple exception to an important cybersecurity protocol can give a hacker access to a law firm's entire network, and potentially its clients' most sacred and valuable secrets.

More and more, reports indicate that these are not isolated incidents. The American Bar Association confirmed that, in 2015, approximately one-quarter of all U.S. law firms with 100 or more lawyers had experienced a data breach through hacker or website attacks, break-ins, or lost or stolen computers or phones. In that same year, 15 percent of all law firms overall, regardless of size, had reported an unauthorized intrusion into the firm's computer files, up from 10 percent in 2012.

These incidents are also quite expensive. The Ponemon Institute found that the typical cybercrime costs a company $8.9 million in operating expenses, lost business and theft of information assets. Lawsuits relating to unauthorized access to personal or confidential business data are also expensive to defend and settle.

Basically, law firms are the next frontier for hackers. Experts agree that many hackers view law firms as one-stop shopping for electronically stored information—accessing both the law firms' information as well as the clients'. And, notwithstanding the greater risks, law firms generally have lower security than most of their corporate clients.

This is the first in a three-part series that will discuss what law firms can do to protect themselves. Part One focuses on the scope of the problem, the risks, and attorney obligations of confidentiality. Part Two will identify common mistakes made by law firms in their cybersecurity practice. Part Three will offer some ideas for how to address this problem and reduce risk.

The starting point is recognizing that law firms are unique targets in that they maintain and store diverse information relating both to clients and employees. Attorneys often falsely assume that no one is interested in their confidential information. However, every attorney and law firm has—in email, document systems or networks—a bevy of confidential information that is valuable to hackers.

This information can relate to confidential business deals, bank account numbers, patent applications or even Social Security numbers (of clients, employees or members of a class). In addition, law firms often obtain sensitive information through discovery that does not relate to their own clients or employees, including trade secrets and insider information. Finally, law firms have trust accounts that contain client money.

While once such attacks seemed to be limited to megafirms with significant overseas practices, that is no longer the case. The growth in web presence for attorneys, through use of internal networks, data storage and personal devices, means that even solo practitioners are vulnerable.

Hacking is not the only risk. Another is the threat to data integrity from malware or viruses. Law
firms also face internal cyberthreats from their own employees, whether those employees intentionally access law firm systems for nefarious purposes, or those employees inadvertently expose the network by losing a laptop or phone, falling victim to a phishing scam or accessing secure law firm networks via an unsecure connection.

For law firms, the protection of information networks and sensitive information residing on those networks is a business and ethical necessity. In addition to the financial risks noted above, law firms also are concerned with ethical and professional duties, violations of which can lead to discipline including suspension from the practice of law to disbarment. Specifically, per ABA Model Rule of Professional Conduct 1.6(c), which was recently adopted, "a lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." This means that attorneys entrusted with confidential or personal data are the guardians of that data.

In evaluating whether an attorney has violated the rule, the comments to the rule indicate that a series of factors will be considered, including the sensitivity of the information, whether additional safeguards would have protected the data and how expensive implementation of safeguards would have been. It is clear that law firms cannot ignore the issue.

Separately, courts have permitted suits against companies that were supposed to safeguard confidential or private information and protect it from hackers. It is not unreasonable to think that law firms, which regularly receive and store confidential data—whether it is details of a proposed merger or client records being reviewed in connection with litigation, or confidential business information needed for a counseling matter—could be held to a similar standard.

Step One: Recognize the risk and do not put it off until another day. The time to act is now.

J. Randolph Evans and Shari L. Klevens are the authors of "Georgia Legal Malpractice Law," published by Daily Report Books.

J. Randolph Evans is a partner at Dentons US in Atlanta. He handles complex litigation matters in state and federal courts for some of the largest companies in the world, and is a frequent lecturer and author on the subjects of insurance, professional liability and ethics. Shari L. Klevens is a partner and deputy general counsel at Dentons US in Washington and Atlanta. She is co-chair of the global insurance sector team, a member of the firm's leadership team and is active in its women's initiative.