The Legal Intelligencer

Page printed from: *The Legal Intelligencer*

Peter F. Vaira

Eastern District

# Protecting Law Firms From Increasing Cyberattacks

Peter F. Vaira, The Legal Intelligencer

June 17, 2014

Cyberattacks are increasing at a startling rate in the business community, not only by hackers for personal intellectual skullduggery, but cyberattacks aimed at obtaining sensitive information that is the heart of the operation of industrial corporations, banks, brokerage houses, and worldwide sales organizations. Law firms have become major targets of these illegal attacks, which are aimed at discovering and pilfering the entire subject matter of a commercial operation. One example is the corporate snooper who will use cyberespionage in an M&A transaction to understand what the competitors are bidding. As discussed below, quite often, such cyberespionage is never discovered or not until a long time after the transaction is completed.

Why law firms? Law firms are frequently consulted by clients on business mergers, marketing and competition strategy, patents, and sensitive problems with government regulators, and possible civil and criminal suits with federal and state regulators. They routinely possess a large quantity of documents and materials that a client's unscrupulous competitor would be eager to see and use. And, they are far easier targets of a cyberattack than their business clients.

Why easier targets? Law firms by their nature do not have the disciplined organizational structure that business organizations possess. Business clients usually have better security than the law firms. Although firms have more corporate characteristics, with committees and practice groups, they are still partnerships with one group of people who are more or less equal. There is usually no firmwide overall discipline for protecting access and transmission and receipt of sensitive material. Partners continue to work weekends and nights away from the office on laptops, and communicate with associates and clients via email. Senior partners talk a big game about security, but experts in cybersecurity view law firms as subject to easy penetration. Cybersecurity is a necessary subject matter for law firm management to confront for two reasons: clients are asking for serious demonstrations of law firms' top-level cybersecurity in many instances and for self-protection in the event that a cyberattack is successful.

Cyberexperts describe two areas that are the most vulnerable to attack: the transmission of material from the client to the law firm or from the firm to the client, and the security of the storage of the material at the law firm. The transmission of information from the client to the firm is done in great part by email transmission of documents, email conversations, and oral communications by telephone. According to Dave Reis of the investigative firm Cloud, Feehery & Richter, the email and oral transmissions are by far the easiest to penetrate by cyberthieves. Sensitive material sent by email should be properly encrypted prior to being transmitted; likewise for email conversations about the material. Lawyers and clients should not pretend they are in some 1940s spy movie and attempt to talk in code. That is the easiest for a professional hacker to interpret. There are encryption software packages available, but don't skimp, and simply turn it over to the office IT manager. Professional assistance is necessary to work with the firm to identify and determine its policies and requirements, and to strike a balance between security and ease of use. This will greatly assist firms in selecting the most appropriate encryption solution. In addition, clients will also need to appropriately encrypt their email communications and attachments to ensure security throughout the communication cycle.

Firms and clients will soon realize that they cannot always deal with each other by encrypted emails and personal meetings are not always possible, especially in fast-breaking situations. Oral conversations by phone are the easiest to penetrate. There are differing opinions whether speaking with a client over a cellphone about confidential client matters is a violation of attorney confidence standards. Regardless of whether such communications are legally acceptable, as a practical matter, lawyers must often speak to clients about sensitive matters on an urgent basis. There is one solution that will protect the integrity of the communications if simple rules are followed. According to Reis, the lawyer and the client should each purchase a $15 cellphone from Walmart, pay for them in cash, and exchange the phone numbers. Even the FBI cannot penetrate such an arrangement. After two months, the phones should be destroyed, and new phones purchased with new phone numbers. Only a specific lawyer and specific client contact should use the phones.

What should be done to protect client product once received by the firm? Protecting the data when stored at the law firm is a more complex problem. The people who are permitted access to the file must be limited, and a provision must be made for recording every entry to the file. Thus, the partner in charge of the file is responsible for assigning the associates or junior partners who have access to the file. Secretarial access to the material for typing and copying must be recorded. In the case of a breach, the firm will be responsible for demonstrating all people who had access in an attempt to find the leak.

The first step is to determine the overall security posture of the firm. A qualified expert must conduct a comprehensive "vulnerability assessment" in accordance with industry guidelines and standards. This assessment should identify weaknesses in the information system, security procedures, processes and internal controls. The assessment should also provide an actionable plan to mitigate risks while minimizing disruption to the firm's work, personnel and resources. A firm should employ a "defense-in-depth" approach to securing its data and networks to determine if there are any possible points of failure in its system. Once again, this should be performed by trained experts. Access to the files should be restricted. Servers and systems should run only the most current versions of the software. Once these mitigation measures are in place, periodic audits should be conducted to measure the firm's vulnerability and to test a firm's detection and response capacity.

The internal storage program should then be given a test that will most likely turn off major partners from the old school: a pentest, an independent, planned cyberattack intended to penetrate the firm's security system. Pentests are an important component of any approach to vulnerability assessments. In short, this is done by the cyberexperts you hire to see if they can steal your client material. This should only be done with trained professionals. Pentests should be thoroughly planned, clearly communicated to and approved by appropriate stakeholders. Once the results of a pentest are compiled, mitigation measures should be implemented, and vigilance maintained to monitor new and emerging threats.

How can firms monitor to see if there was intrusion? Security breaches aren't always detected. An intrusion doesn't necessarily mean the information is stolen in the manner of removing the document. It is often copied, leaving no visible trail of the intrusion. Often the victim, law firm or client, is unaware of the breach for months or years. A set of regular tests should be performed in this process. There are commercial programs available to assist firms in investigating and tracking suspected incidents. These tools can be customized to verify and correlate attacks. Once again, these should be installed and operated by outside experts.

What steps must be taken when intrusion is discovered? Notify the client. Although there has been discussion among legal commentators whether a client should be notified of such a breach or possible breach, partners at a law firm would be rolling dice with their malpractice carrier and their own careers if the client was not informed immediately. Clients may be able to assist in verifying the damage or the possible perpetrators. Rule 1.1 and Rule 1.6 of the Model Rules of Professional Conduct state that a law firm has a duty to effectively protect their client's information. The Restatement of the Law Governing Lawyers provides that if the lawyer's conduct gives a client a substantial malpractice claim, the lawyer must disclose the matter to the client.

What personnel or administrative action should the law firm take upon discovery of a possible breach? In the event a firm is breached, a firm should have an incident response plan in place, with attention to technical aspects and the law firm's duty to its client and responses to the media. The plan should include who is in charge, and who has the responsibility to speak about the incident (both publicly and to clients). As for responses to the media, start with this rule: don't. It is the client and its material you must protect. Make an immediate report to the FBI with as much technical detail as possible.

There should be clearly defined roles, responsibilities, and lines of communication for an effective incident-response capability. Once an incident is detected, the firm should have expert advice as its response in accordance with defined policies, procedures and timeframes depending on the nature/severity of the threat. A practical step is to have one person be the action person to perform these steps. This should be an expert consultant or a person designated by the outside expert consultant as the person in charge. A firm's post-incident actions should include follow-up assessments to ensure the implementation of mitigation measures. In other words, test again. This will include training to ensure awareness of threats, and changes to firm procedure.

The firm's vulnerability to lawsuits: There is little law or comment on this subject as yet. The standards for protecting material from hackers or cyberpirates is not clear, although some client firms have required law firms to install special systems to guard against such attacks.

Rest assured a case of this nature is sure to be filed. The Chubb Group of Insurance Cos. has advertised a special malpractice type of policy for cyberattacks.

In summary, this cyberattack protection is a subject that will eventually involve almost all firms with substantial business clients. Midsized firms, as well as giant firms, are handling matters for international clients, which increases the chances of cyberattacks. Law firm leaders can no longer say turn it over to the IT people. The management of the firm must be involved with one key partner as a cyberperson. Ken Gormley, dean of Duquesne University School of Law, said, "Law schools, too, now understand that it is crucial to educate students about the importance of specialty services provided by privacy and data security attorneys."

What happened to the old days when lawyers practiced law, partners specialized in their specific discipline, associates wrote memos and sent them to partners, secretaries kept files, and everyone went home at night knowing the office was secure? A time long past.

***Peter F. Vaira** is a member of Greenblatt, Pierce, Engle, Funt & Flores. He is a former U.S. attorney, and is the author of a book on Eastern District practice that is revised annually. He can be contacted at p.vaira@gpeff.com.* •

---