Safeguarding your firm from cyber attacks
Law Firm Services

Law Firm Services

Dedicated to serving law firms and their partners

At a glance

Cyber attacks against law firms are on the rise.

For international law firms, the greatest threat comes from well-funded hackers seeking information on clients' pending deals and litigation.

To protect their data and reputation, law firms need to make sure their cyber defenses keep pace with ever-evolving threats.

pwc

Introduction

Law firms are growing increasingly aware that they are being targeted by cyber criminals intent on stealing their clients' secrets. A series of breaches at major international firms has convinced many of them to strengthen their defenses. They are also finding that enhancing security controls[1] and storing client information on the firm's network are becoming prerequisites for doing business.

1 For instance, by installing data-loss-prevention technologies that "tag" certain files, phrases, and code names that the law firm would like to block, with the aim of preventing sensitive information from leaving the firm's network

Notice to law firms: Hackers want your secrets

Despite their heightened alertness to data security, a number of law firms believe they are too small or obscure to warrant the interest of professional hackers. They may want to rethink that logic. A fraud alert issued by the FBI last spring warned that cyber criminals had begun to aggressively target small and midsize businesses,[2] and in July the *Wall Street Journal* reported that there had been a sharp increase in data breaches among companies with 100 or fewer employees. "Hackers are expanding their sights beyond multinationals to include any business that stores data in electronic form," the *Journal* said.[3]

"There is no question that law firms are among the companies being targeted by cyber criminals," says Shane Sims, a director in PwC's Forensic Services group. Mary Galligan, head of the cyber division in the New York City office of the FBI, agrees: "As financial institutions in New York City and the world become stronger, a hacker can hit a law firm and it's a much, much easier quarry."[4]

Sims notes that cyber criminals come in many stripes, and all of them are looking for an easy score. While some hackers may want only to steal an unwary partner's online banking credentials, others have much more ambitious goals.

A key threat, according to the US government,[5] comes from foreign intelligence agencies looking to learn the plans of major corporations that are making large investments, contemplating joint ventures, or considering acquisitions.

"Many states view economic espionage as an essential tool in achieving national security and economic prosperity," notes a report on cyber crime that the Office of the Director of National Intelligence presented to Congress in 2011.[6] The report goes on to say that such espionage "includes computer network intrusions and exploitation of insider access to corporate and proprietary networks to develop information that could give these states a competitive edge over the United States and other rivals."

2 China Wire Transfer Fraud Alert, Federal Bureau of Investigation, April 26, 2011

3 "Hackers Shift Attack to Small Firms," *Wall Street Journal,* July 21, 2011

4 "China-Based Hackers Target Law Firms to Get Secret Deal Data," *Bloomberg,* January 31, 2012

5 *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage,* October 2011

6 Ibid

Organizations involved in cyber crime are well funded, extremely sophisticated, and relentless. And they grow more so every day.

Law firms are not immune to these threats, as highlighted in a panel discussion hosted by the American Bar Association last year—Foreign Espionage Targets the Private Sector: The Cybersecurity Threat from Nation States—and in a related article published by the *ABA Journal*.[7] Once the law firms involved in a deal are identified, their computer defenses are attacked, along with those of the corporations.

Whether criminal hackers are acting on their own, at the behest of intelligence agencies, or for corrupt corporate competitors, they are not just looking for personal information and credit card numbers; they are after any kind of intelligence that has economic value. "It's imperative to understand that the organizations involved in cyber crime are well funded, extremely sophisticated, and relentless," Sims says. "And they grow more so every day."

Data on the growth of cyber crime is largely anecdotal and piecemeal. Few companies that have experienced an information-security breach are willing to talk about it, although some high-profile companies have nonetheless ended up in the news as a result of well-publicized attacks in recent months.

What companies *have* willingly revealed is that information security is becoming a priority for them. Among private businesses in particular, information security is the top area of planned IT investment, according to PwC's *Trendsetter Barometer* survey.[8] And PwC's *2012 Global State of Information Security Survey* found that among medium-size US companies, a written privacy policy is in place at 68% of them, and 63% require their employees to certify in writing that they're in compliance with the company's privacy safeguards.[9]

There is no way to predict the likelihood that any given law firm will be attacked, says David Gaulin, co-leader of PwC's Law Firm Services, but the consequences of a security breach are obvious and painful: "Privacy and confidentiality are bedrock qualities for law firms. The theft of client information could be devastating to a firm's reputation, which is their most important asset."

7 "Law Firms Overlook Vulnerabilities to Cyberattacks," *ABA Journal,* August 6, 2011

8 *Trendsetter Barometer: Private Companies Rebuild IT Budgets,* PwC, June 2011

9 *2012 Global State of Information Security Survey,* PwC, September 2011

Where firms are vulnerable

"Many law firms are moving to strengthen their defenses," says Gaulin. He stresses that the most sophisticated hackers do not try to penetrate a firm's perimeter defenses, such as firewalls. Instead, they target personal workstations through email, hoping that a careless or distracted employee will click on a bogus link, allowing the hacker entry. This poses a widespread risk, considering the size of law firms today and their diverse operations.

"End-user computers are the weakest spot in most companies' systems," says Sims. "Typically, these computers are protected only by antivirus software, and the most sophisticated hackers attack at that point rather than try to work their way through a web server or other external-facing protections."

If a hacker has penetrated the network of a law firm's client and stolen the email of in-house counsel, for example, it's then easy to identify the email addresses of outside attorneys and to fabricate messages that deceive people at the law firm.

Companies that rely heavily on communications technology frequently hire outside experts to test the security of their networks. These outside firms, called "ethical hackers," are usually able to penetrate internal networks. Sometimes they do this by the simplest means, such as phoning employees, claiming to be internal IT staffers, and then asking for a password. Or they gain entry to the office and steal laptops or paperwork that serves as a giveaway.

Once cyber criminals gain access to a computer system, they typically have the ability and desire to stay there and hide. Their goal is not to snatch information and flee, but to remain secretly entrenched, monitoring the information flow and harvesting ever more valuable intelligence. Hackers can maintain a presence in corporate systems for many months without detection, unless a firm takes proactive measures.

Privacy and confidentiality are bedrock qualities for law firms. The theft of client information could be devastating to a firm's reputation, which is their most important asset.

What firms can do

So prevalent is hacking that PwC's advice to major organizations (law firms included) is to assume that their systems have been compromised and then proceed from that assumption in testing and improving their defenses. We recommend that, at a minimum, all law firms consider taking six basic actions:

1

Make sure leadership is sensitive to the threat and aware of the importance of constant vigilance. Leading law firms ensure this by making one or more senior partners responsible for IT activities or by establishing an IT committee of partners. These approaches provide an open communications channel from the IT people to senior management and ensure that data security has the attention of the highest levels of management.

2

Install antivirus programs that protect against known viruses. To be effective, these programs must be centrally managed and updated regularly.

3

Continually update spam filters. Such filters need to be kept current if they are to do an adequate job of intercepting unwanted or suspicious email.

Smart moves

42% of medium-size US companies that participated in PwC's *2012 Global State of Information Security Survey* say they've instituted controls for copying company data to external devices such as USB drives.[10] Indeed, a number of firms require employees who are traveling or working at home to use a virtual desktop provided by the company rather than load data into their laptops or workstations. When the employee logs off, the desktop disappears, and nothing is stored in the computer.

10 *2012 Global State of Information Security Survey,* PwC, September 2011

4

Run an analysis program that detects unusual behaviors, activities, or programs in the system. These programs, often called host-intrusion protection (HIP), are necessary because hackers frequently develop special malicious software (malware) that antivirus programs are unable to detect.

5

Develop a response in case the firm's systems are violated. This should consist of a plan regarding whom to notify if a breach occurs, as well as what actions to take to protect the data, determine who violated the system (and how), and minimize the damage and disruption to the firm.

6

Institute ongoing training programs. It is important that all partners and staff become sensitive to the threat of an information-security breach and be educated in what they can do to prevent or detect it. A culture of awareness should therefore be developed in the firm via ongoing training programs and best practices aimed at protecting information.

These and other defenses against cyber crime are constantly evolving to keep pace with the techniques of criminals, and no one in the field expects that to change. "The miracles wrought by computers and communications technology can be used for good purposes or bad ones," said Gaulin, "and they always will be."

www.pwc.com/us/lfs

To have a deeper conversation about how cyber security may affect your business, please contact:

David Gaulin
Partner
Law Firm Services
646 471 1810
david.gaulin@us.pwc.com

Shane Sims
Director
Forensic Services
703 918 6219
shane.sims@us.pwc.com