On Jan. 2, agents of the FBI arrested 19-year-old Igor Serebryany at his parents' home in Los Angeles. The FBI alleged that he stole confidential documents from DirectTV Inc. that could help a hacker pirate the satellite provider's signal and posted those documents to the Internet. He faces up to 10 years in prison and potential fines of up to $250,000.

The FBI said Serebryany will be charged and prosecuted under the 1996 Electronic Espionage Act. It makes economic espionage and theft of trade secrets crimes punishable by fines, prison time or both. The act's definition of each gives the law a distinctive digital flavor.

This arrest is the latest in the ongoing war between DirecTV and the pirate "community" that keeps trying to sabotage its scrambled signals. But there's another reason why the legal tech community needs to monitor this case: It happened on home turf.

The alleged theft occurred at the Los Angeles office of Jones Day Reavis & Pogue, at its imaging center, outsourced to Uniscribe, a professional services company that specializes in litigation support. According to FBI documents, Serebryany reportedly copied 800 MB of data onto two compact discs and used the firm's copy center computers to search for Web sites used by hackers eager to pirate satellite service. Jones Day client DirectTV was in a civil dispute concerning, ironically, misappropriation of company secrets.

Serebryany's attorney, federal public defender Charles Brown, has declined to comment on the matter. Jones Day spokesman Paul Engle is not commenting at this time.

But Uniscribe president and CEO Ronald Self is talking. Self said his company and the law firms it works with have learned important lessons from the incident.

"It's an unfortunate circumstance," said Self, of the Jones Day incident. "We have 1,300 employees, and we had three employees on that site. [Serebryany] wasn't even an employee, he was brought in by our person to help in a crunch."

Jones Day and Uniscribe's other client-firms have been nothing but supportive and sympathetic, Self said. Everybody recognized that it was a situation "that could happen to anyone."
Uniscribe continues to work with Jones Day. "Obviously, we're not running their imaging facility in L.A. where breach occurred, but we are still partnering with them in L.A. [on other matters] and at other offices," Self said.

Uniscribe immediately started audits at its 55 law firm sites and has launched "very constructive discussions" with Jones Day and other client-firms about how to beef up security to prevent future breaches. Changes have taken place immediately. For example, Jones Day and other firms have installed firewalls with tight authority levels that limit access to firm information to authorized employees.

The Electronic Espionage Act isn't limited to criminal remedies against individuals. Organizations can be prosecuted as well and, if convicted, fined up to $5 million - for each offense! While no one has suggested that Uniscribe or Jones Day should face criminal prosecution in this case, the incident does draw attention to a number of questions that could arise when companies - or law firms - process electronic data discovery requests.

Wise firms and vendors should take a cue from this incident and consider the following questions:

* Are you vulnerable in a civil action for negligence claims over document processing?
* How likely is it that a "corporate hacker" would attempt direct network intrusion of a law firm or engage in "social engineering" to gain access to valuable client information?
* How are vendors screening their employees, especially temps?
* What else should be done, besides firewalls and proxy servers, to safeguard valuable electronic information?

Christopher Brown is a reporter for Law Technology News, an affiliate of the Daily Business Review.

LOAD-DATE: March 05, 2003