



LJN'S

# LEGAL TECH

Newsletter®



Volume 25, Number 1 • April 2007

## Protecting Your Firm Against Internet Threats

### *Strategies to Detect and Fight Cyber Crime*

By Christy Burke

Everyone today is on high alert about the threats of Internet fraud, identity theft and white-collar crime — or if not, they should be. Internet criminals are constantly cultivating new tactics, and law enforcement entities are doing everything they can to head them off.

At New York Legal Tech in January, the opening keynote address was given by David Thomas, chief of the FBI CyberDivision's Criminal Intrusion Unit. In his presentation, Thomas detailed the growing industry of cyber crime from sources in Eastern Europe, China and India. Artwork to create counterfeit credit cards (MasterCard, Visa, and AmEx) can easily be bought on the Internet. Lists upon lists of "fuls," which include an individual's full personal ID information including social security numbers, mother's maiden name and credit card numbers, are easily available for purchase on Internet sites.

"Why aren't these thieves being locked up?" you might ask. Thomas explained that the governments of the criminals' host countries often do not actually outlaw this kind of activity. In fact, the industry has become so legitimized in certain countries that publicly distributed magazines contain "how to" instructions on perpetrating these crimes. Thomas's message to the awestruck Legal Tech audience: "It's not a question of *if* identity theft will happen to you — it's a question of *when*."

After the Legal Tech keynote, many of the attendees expressed shock at the easy and cheap access to valuable and potentially damaging personal information on the Internet. If identity theft is so staggeringly widespread and private information so easily obtained, what greater ramifications does this have for the security of law firm data and electronic property?

Both law firms and businesses can attest that the cost of doing business has increased exponentially as high-tech security hardware, software and personnel have become necessary to protect the average company's day-to-day operations. Wireless Internet connections, as well as wireless devices such as cell phones and PDAs are all necessary for today's mobile lawyering, but we forget that they are all hackable and present exposure risks. And with so many lawyers breaking off from their mother ship law firms, the possibility of theft of files, contacts, trade secrets and intellectual property represents a huge exposure.

Understandably, concerned attorneys and law firm IT managers want to know where these threats are coming from so they can properly arm themselves.

#### **PROTECT AGAINST EXTERNAL THREATS**

Above all else, law firms need to protect their primary product — their data. Factories manufacture widgets; law firms produce documents and e-mail. While the large law firms have been setting the pace in protecting their electronic property, many smaller firms are facing the reality that external Internet threats are not going away.

"An adequate firewall and Internet router is essential for all law firms — large or small," says Brian Cluxton, IT Manager at HMU Consulting, an IT consulting firm that specializes in working with law firms. Cluxton explains that surprisingly, many law firms he works with, most of which have less than 100 attorneys, either don't have a firewall at all or they are using an inadequate firewall that is designed for home rather than business use. Cluxton recommends that, above all else, every firm's firewall should include SPI — Stateful Packet Inspection. SPI inspects each packet of incoming information to make sure the file actually is what it says it is (e-mail, FTP, Internet, etc). One of the ways in which cyber criminals disguise malicious files is by spoofing e-mail domains that are familiar to the user. When unsuspecting users open these files, they can unwittingly unleash viruses and spyware on their computer, and possibly on the whole firm. SPI examines e-mails and other network traffic and rejects data that is potentially dangerous.

#### **EXAMINE THE INTERNAL SECURITY THREATS**

In addition to staving off menacing threats from external sources, many of today's Internet crimes are increasingly originating from within a lawyer or executive's "circle of trust."

IT staffers themselves represent a huge exposure for companies and law firms alike. Think about it — the IT people know the master passwords and the vulnerabilities of the network and security system.

Take for example the *United States v. Roger Duronio* case that took place in the summer of 2006.

Duronio was a Systems Administrator at UBS Paine Webber who became disgruntled due to salary and bonus issues and resigned in 2002. Before he left the firm, Duronio planted a "Logic Bomb" containing malicious computer code that shut down approximately 2000 servers and 15,000 desktops simultaneously.

One of the prosecutors on the case was Mauro Wolfe, an Assistant U.S. Attorney at the time and now a Partner at Dickstein Shapiro LLP. Wolfe says that the Logic Bomb code was designed to cripple the company's brokerage business, and was timed to detonate only after Duronio had exited the company. UBS PaineWebber's cost to remedy the problem was approximately \$3.1 million.

Was Duronio a computer genius? Wolfe says not necessarily, remarking that a high-school sophomore would have the programming skills to put together the Logic Bomb code from a computer class. However, unlike your average high school student, Duronio was familiar with the company's systems; he knew the security's strengths and weaknesses. He exploited this insider information to disable the system and bring business to a standstill. The *Duronio* case shows that large-scale damage can be done with a moderate skill level, and that any kind of company can be at risk of a similar crime if it doesn't take proper precautions. Think of what would happen if all of your law firm's servers and workstations crashed at the same moment. What would you do?

#### **HAVE A CRISIS MANAGEMENT PLAN**

Inspired by his work on the *Duronio* case, Wolfe set out to answer the question of what to do in

**Christy Burke** is a freelance writer who focuses on legal technology issues. She has previously been published in the *e-Discovery Law & Strategy*, the ABA's *Law Practice Today*, and other leading legal and technology journals. She can be reached at [cburke@burke-company.com](mailto:cburke@burke-company.com) or 917-623-5096.

the event of cyber-sabotage at your firm or organization. He delivered a presentation (also at New York Legal Tech 2007) about critical lessons in-house counsel should know before a computer attack hits the company. He feels that many companies and firms are still not taking these threats seriously enough, despite overwhelming evidence of their likelihood. Wolfe notes that many companies tend to focus mostly on purchasing security hardware and software geared toward warding off *external* security threats rather than protecting against *internal* malfeasance. Some firms spend enormous sums on their firewalls, but they underestimate or ignore the considerable risks of an "inside job."

Wolfe recommends that every company and law firm have both a Crisis Management Plan and Team in place. A Crisis Management Team can include recovery specialists, investigators and law enforcement contacts and a future prevention group that consists of computer intrusion prevention specialists and IT security professionals.

In the event of an act of sabotage such as the Logic Bomb case, Wolfe says your firm's Recovery Group can consist of IT personnel, internal staff, incident response experts, your computer hardware and software vendors, and archive data resources. Having these diverse perspectives integrates all the different parts of a company to deal with intrusion incidents. Wolfe recommends a series of plans, procedures, tests and "fire drills" that the team runs through to maintain its rigorous dedication to securing the company and its data. Wolfe admits that there is virtually no way to make a system 100% security-proof, but having the right security and personnel in place to prevent and crack down on illegal activity is a solid approach.

#### **LOCK DOWN VULNERABILITIES**

Given the risks posed by today's Internet-dominated environment, law firms cannot afford to ignore or underestimate these risks. In addition to the aforementioned robust firewall, Cluxton recommends that a firm have anti-virus protection on servers and

workstations, keep Windows updates current, and have anti-spyware protection in place. He also stresses the need for law firms to put in place stringent policies for its attorneys and staff, and then enforce those policies rigorously.

Attorneys' remote access to documents must be locked down and controlled carefully for laptop and home-based users. Cluxton recommends that attorneys only be allowed to access documents off of the firm's server via a VPN where the traffic is encrypted — not by loading documents onto their own laptop hard drive or accessing them via an unprotected Internet connection. There is huge risk associated with allowing attorneys to access data via unprotected wireless connections from home, or perhaps worse, from an airport or coffee shop where anyone sitting nearby can have access to the firm's network and documents.

#### **WHEN ATTORNEYS LEAVE THE FIRM**

If your firm suspects that a lawyer, or group of lawyers, is getting ready to leave the firm, the network administrator can cut off their access to documents immediately, which prevents them from copying files illegally. Barron Henley, President of HMU Consulting, says that legal software can also be useful in preventing lawyers from stealing files without the firm knowing about it. Henley says that firms that have a document management system (DMS), such as WORLDQX, can restrict rights and access to documents. Most of them also have an audit trail that can tell the IT staff what actions were done with a given document — whether it was opened, copied, edited or deleted. Henley also says that document assembly software, such as HotDocs Pro, can be set up with a 30-day fuse so the software expires after a month if the attorney is no longer privy to the firm's network. Henley explains that the HotDocs component file can also be locked, rendering the HotDocs templates useless. This is another way to prevent lawyers from taking firm files with them when they leave.

Upon first suspicion that an attorney might be leaving the firm, pass-

---

words need to be changed immediately — not only that of the departing lawyer but also that of others in the lawyer’s practice group and staff as well. Cluxton reports that at some overly trusting firms, all or several of the users have the exact same password. Therefore, when people leave the firm, they can still get access even though they are no longer physically at the firm. Clearly, a law firm’s password system has to be complex and possibly multi-layered to be truly useful. Cluxton recommends that firms encourage, or even

force, their users to change their passwords frequently so that if a user password gets “out in the open,” the damage will be minimized.

There are also software products on the market that allow IT personnel to surreptitiously monitor users’ workstations without their knowledge. Products such as Spector CNE can be silently installed on the user’s PC. This software can log which files have been opened or copied, and record what’s been typed on the keyboard.

With great technology comes great responsibility — this is the

world we live in now, like it or not. The threats are significant and scary, yes, but the smartest firms and legal departments can arm themselves with the right products, procedures and policies to keep them out of the path of the cyber-hurricane.



**The publisher of this newsletter is not engaged in rendering legal, accounting, financial, investment advisory or other professional services, and this publication is not meant to constitute legal, accounting, financial, investment advisory or other professional advice. If legal, financial, investment advisory or other professional assistance is required, the services of a competent professional person should be sought.**