

Shield Your Firm From Cybercrime

Software and Procedures Diligently Applied Can Help Companies and Law Firms Protect Themselves

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 agencies are doing everything they can to head them off.

At New York LegalTech 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 cybercrime from sources in Eastern Europe, China and India. For instance, artwork to create counterfeit credit cards (MasterCard, Visa and AmEx) can easily be bought on the Internet. Lists of "fulls," 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 don't 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 how to perpetrate these crimes. Thomas' message to the awestruck LegalTech audience: "It's not a question of *if* identity theft will happen to you — it's a question of *when*."

After the LegalTech keynote, many 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, then what greater ramifications does this have for the security of law-firm data, e-commerce ventures' information and electronic property?

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 can all be hacked 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 that they can properly arm themselves.

PROTECT AGAINST EXTERNAL THREATS

Above all else, law firms must 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," Brian Cluxton, IT manager at HMU Consulting, an IT consulting firm that specializes in working with law firms, says.

Cluxton explains that, surprisingly, many law firms he works with, most of which have fewer than 100 attorneys, either don't have a firewall or are using an inadequate firewall designed for home rather than for business use. Cluxton recommends that every firm's firewall should include stateful packet inspection ("SPI"). SPI inspects each packet of incoming information to make sure that the file is what it says it is (e-mail, FTP, Internet). One of the ways that cybercriminals disguise malicious files is by spoofing e-mail domains 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 potentially dangerous data.

EXAMINE THE INTERNAL SECURITY THREATS

Besides staving off menacing threats from external sources, many of today's Internet crimes more often originate from within a lawyer's 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 network and security-system vulnerabilities.

Take for example the *United States v. Roger Duronio* case from last summer. Duronio was a systems administrator at UBS Paine Webber disgruntled over salary and bonus issues who resigned in 2002. Before he left the firm, Duronio planted a "logic bomb" containing malicious computer code that shut down about 2000 servers and 15,000 desktops simultaneously.

One of the prosecutors on the case was Mauro Wolfe, then an Assistant U.S. Attorney and now a partner at Dickstein Shapiro. Wolfe says that the logic bomb code was designed to cripple the company's brokerage business, and timed to detonate only after Duronio had exited the company. UBS PaineWebber's cost to remedy the problem was about \$3 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. But unlike your average high school student, Duronio knew the company's systems, and 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 moderate-level skill, and that any kind of company can be at risk of a similar crime

Christy Burke is a New York City freelance writer who focuses on legal technology issues. She has been published in our sibling publication, *e-Discovery Law & Strategy*, the ABA's *Law Practice Today*, and other leading legal and technology journals. Reach her at cburke@burke-company.com, or 917-623-5096.

if it doesn't take proper precautions. Think of what would happen if all 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 the event of cyber-sabotage at a firm or organization. He delivered a presentation (also given at New York LegalTech 2007) about critical lessons that in-house counsel should learn before a computer attack hits the company. He feels that many companies and firms are still not taking these threats seriously, despite overwhelming evidence of the likelihood of them happening. Wolfe notes that many companies tend to focus 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 a crisis-management plan and crisis-management team in place. A crisis-management team can include recovery specialists, investigators and law-enforcement contacts, plus a prevention group that consists of computer-intrusion prevention specialists and IT-security professionals.

In the event of sabotage such as in 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 data-archive resources. Having these diverse perspectives integrates all the different parts of a company to deal with intrusions. Wolfe recommends a series of plans, procedures, tests and "fire drills" for the team to run through to maintain its rigorous dedication to securing the company and its data. Wolfe admits that there's virtually no way to make a system 100% secure, but having the right security and personnel in place to prevent and crack down on illegal activity is a solid approach and a good start.

LOCK DOWN VULNERABILITIES

Given the risks posed by today's Internet-dominated environment, law firms cannot afford to ignore or underestimate them. Along with a robust firewall, Cluxton recommends that a firm have antivirus protection on servers and workstations, keep Windows updates current, and have antispyware protection in place. He also stresses the need for law firms to put in place stringent policies for attorneys and staff, and then enforce those policies rigorously.

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

WHEN ATTORNEYS LEAVE THE FIRM

If someone suspects that a lawyer, or group of lawyers, in your firm is getting ready to leave, the network administrator can immediately cut off access to documents that the person or people might have, which prevents illegal file-copying.

Barron Henley, president of HMU Consulting, says that legal software can also be useful in preventing lawyers from stealing files without the firm knowing. Henley says firms that have a document-management system, 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 — such as whether it was opened, copied, edited or deleted. Henley also notes that document-assembly software, such as HotDocs Pro, can be set up with a 30-day fuse so that 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 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, passwords need to be changed immediately — and not only the password of the departing lawyer, but also of others in the lawyer's practice group and staff. Cluxton reports that at some overly trusting firms, all or several of the users have the same password. So, then, when people leave the firm, they can still achieve access

even though they are no longer physically at the firm. Clearly, a law firm's password system has to be complex and possibly multilayered to be truly useful. Cluxton recommends that firms encourage, or even force, users to change their passwords frequently so that if a user password gets "out in the open," the damage will be minimum.

Some software on the market allows IT personnel to monitor users' workstations without their knowledge. Products such as Spector CNE, for instance, 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, like it or not. The threats are significant and scary, but the smartest firms and legal departments can arm themselves with the right products, procedures and policies to ward off and stop cyberthieves in their tracks.



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.