The Federal Lawyer in Cyberia

by Mike Tonsing

The Cyberian World Grows Colder Every Day. Cybercrime Abounds. Consider Building a Few Igloos to Protect Your Firm from the Frost.

Savvy Cyberian lawyers know that "cybercrime" is one of the fastest growing areas of law breaking worldwide. We're all aware of headline-grabbing articles about successful efforts to hack into Department of Defense computers. And, most of us know about the growing concern among governmental officials that cyber terrorists, foreign intelligence services, or other groups are organizing these efforts to map potential security holes in our nation's most critical databases and systems.

However, not all such hackers are politically motivated. More and more anarchists and criminals—motivated primarily by anti-societal feelings or garden-variety greed—are exploiting the speed, convenience, and anonymity that modern technology offers to engage in an amazingly wide array of criminal activities.

In the past, cybercrimes seemed to be the province of thrill-seeking nerds and small, isolated groups of "cottage industry" thieves. Not today. A new and frightening trend is emerging, as traditional organized crime syndicates and criminally minded technology professionals pool their expertise, directing their efforts toward stealing all sorts of things that have intrinsic value.

According to a report in the *Los Angeles Times*, LinkedIn™ and eHarmony™ were attacked in early June of 2012, compromising roughly 65 million passwords. The hackers cracked 30,000 passwords and publicly shared 1.5 million of them from eHarmony.

In December 2012, Wells Fargo Bank's website experienced a denial of service attack, as reported by *Reuters*. The hackers behind the attacks on this quintessentially private enterprise target used sophisticated and diverse tools that pointed to a carefully coordinated campaign. Then U.S. Defense Secretary Leon Panetta called its scale and speed "unprecedented," urging Congress and businesses to step up their cybersecurity efforts in a speech delivered shortly after the attack. This attack is said to have potentially compromised the confidential information of an estimated 70 million customers of the country's fourth-largest bank. Experts posit that institutions including Bank of America, JP Morgan, U.S. Bank, and PNC Financial Services may also have been compromised at about the same time.

Not all such domestic attacks have been directed against banks, of course. According to the *New York Post*, a "cyberthief tiptoed into the virtual world of retail shoe giant Zappos and ripped off 24 million customer names, email addresses, and phone numbers" in January 2012. (Zappos, with its distinctive branding and emphasis on customer service, is one of the nation's largest online retailers and was purchased by Amazon for $1.2 billion in November 2009.). This online security breach also garnered personal information, billing and shipping addresses, and the last four digits of their credit cards. The hackers apparently targeted a company server in Kentucky, according to Zappos CEO Tony Hsieh.

"We've spent over 12 years building our reputation, brand, and trust with our customers," he told the *Post*. Hsieh reportedly wrote to employees shortly after learning of the cybertheft. "It's painful to see us take so many steps back [in terms of customer confidence] due to a single incident."

Rob Holmes, the CEO of high-tech detective agency IPCybercrime.com, told the *Post* he didn't believe Zappos customers' identities were truly in danger of being stolen. And, subsequent events seem to have borne out his opinion. But, Holmes warned at the time that Zappos customers should brace for an increased run of spam.

"The individual isn't the value here—it's the list that's the value," he said in the article. He explained that the stolen email addresses and names would be a hot commodity in the shadowy world of spam middlemen—businesses that buy information and peddle it to online retailers. "This could be the greatest spam list ever compiled. We're talking about 24 million vetted Zappos customers. You know their names and addresses and that they're willing to shop online."

"If it [cyberattacks] happens to countries, to governments, to the CIA, it can happen to a shoe retailer," branding guru and Landor Associates Managing Director Allen Adamson told the *Post* for the same article.

Michael J. Tonsing practices law in San Francisco. He is a member of the FBA editorial board and has served on the Executive Committee of the Law Practice Management and Technology Section of the State Bar of California. See www.TonsingLawfirm.com. He also mentors less-experienced litigators by serving as a "second chair" to their trials (www.YourSecondChair.com). He can be reached at Mike@TonsingLawfirm.com.

Moral of the Story

Small firm lawyers, like large shoe retailers, are not immune.

I am a sole practitioner. I have become aware that cybercriminals have targeted my passworded law firm accounts several times in the past few months. Apparently, each attack focused on hacking into a single, passworded law firm email account rooted in Gmail. Also, apparently, each of these known (and now well-documented) attacks has emanated from a third-world country. But, one cannot discount the possibility that overseas sources have been used to perpetrate thefts supported by domestic sources.

Regardless of the source, a database compromise experienced by a law firm, large or small, could have catastrophic consequences with respect to the firm's ethical obligations and the confidence of its clients. Fortunately, in my case, it appears that the hacking attempts were unsuccessful, but they surely taught me a lesson. Had a breach occurred, it could have been quite serious since I have a habit of using the same password for multiple purposes.

What happened to Zappos could happen to me or you. In fact, the Association of Certified Fraud Examiners recently reported a sobering statistic. Domestic companies with fewer than 100 employees lost an average of $155,000 annually as a result of fraud, identity theft, and cybercrime.

If that statistic doesn't stop you in your tracks, however, I warn you not to be mollified into a false sense of security by the relatively manageable size of that loss, thinking of this as a cost of doing business in today's world. Remember, this figure is only an average, and your firm's loss could be far greater given the nature of the work we lawyers do. If that doesn't concern you, you are not paying attention.

Igloos You Can Build

Here are some practical suggestions for protecting your firm from becoming a Cyberian victim. Most of them will incur little if any intrinsic cost. Not all of them will apply to all firms, but I believe all are worthy of your consideration:

- *Protect bank accounts and credit cards*. First, if you are a sole practitioner, be sure that your personal banking and credit accounts are kept separate from your business accounts. Whatever your firm's size, be stingy when issuing law firm credit cards and paying firm bills online. Use a secure mailbox for sending and receiving mail. It is no longer paranoid to have someone check your firm's bank account balances daily for suspicious activity.
- *Firewall protection*. Protect your firm's computers with a firewall, and install anti-virus, malware, and spyware detection software on every network computer. Have a robust back-up system for all your business data.
- *Dedicated banking computer*. Consider installing a dedicated, freestanding computer for all online banking activities, and make sure it is never used for web surfing or other online activities that could make it more vulnerable to hackers.
- *Password policy*. Invoke a firmwide policy to change passwords every 30 to 60 days. And, use passwords that are random and tough to crack.
- *Educate firm employees*. Educating employees on threats and prevention methods is your best defense. Hold regular training sessions and be sure to educate new hires. Before hiring anyone, conduct a background check to ensure you are hiring the right people—but, of course, ensure that such background checks comply with local laws.
- *Insurance*. Get an insurance policy that protects your firm from any direct firm loss or any liability suit that could arise from cybercrime.

Conclusion

The Cyberian world grows colder every day. Consider building igloos to protect your firm from the frost. See you next time in Cyberia. ⊙