

The Metropolitan Corporate Counsel

www.metrocorp-counsel.com

Volume 18, No. 11

© 2010 The Metropolitan Corporate Counsel, Inc.

November 2010

Virtual Crimes – Real Damages: Challenges Posed By Cybercrimes In The United States

**Fernando M. Pinguelo and
Bradford W. Muller**

**NORRIS, McLAUGHLIN & MARCUS,
P.A.**

Introduction

A dangerous aspect of the Internet Age is cybercrime. As technology advances, so do the criminals. For American businesses and government, the cost of these attacks can be staggering.

“Cybercrime,” a term used to describe criminal activity conducted through the Internet, began almost as soon as the Internet came into being. The schemes have proven dynamic, evolving to meet increased security measures. Today, attacks on businesses include the theft of intellectual property, generating and distributing malware, and other disruptions. Cyber attacks against the federal government can potentially devastate the country’s technical infrastructure or lead to the exposure of classified information. State governments also remain an appealing target, as their computer systems hold vital records.

Profiling the Cybercriminal

Cybercriminals take on many forms. For Americans, the cybercriminal they encounter will likely be a male from the United States. One study found that 76

Fernando M. Pinguelo, a trial lawyer, Partner of Norris McLaughlin & Marcus, and Co-chair of its eDiscovery Group, founded the ABA Journal award-winning eDiscovery blog, e-Lessons Learned – Where law, technology, and human error collide. Bradford W. Muller, an Associate of the firm, practices in its Litigation Group.



Fernando M. Pinguelo

percent of cybercriminals were male, with over half residing in one of nine states or the District of Columbia. While California had the largest share of reported perpetrators, the District of Columbia had the most cybercriminals per capita. Far and away, the United States had the most cybercriminals in the world, with over half of those reported residing in the country. For businesses, besides defending against cyber agents engaging in corporate espionage, they must be wary of “malicious insiders,” disgruntled employees who turn against the company. And for the government, the cyber threats include foreign nations, criminal groups, hackers, hacktivists, disgruntled insiders, and terrorists.

Major Forms Of Cybercrimes Of Which Government And Businesses Are Wary

Corporate or Foreign Espionage

Espionage is a hot topic in the cyber



Bradford W. Muller

realm. In August 2010, the Department of Defense issued a report discussing China’s increased focus on developing viruses to attack foreign computer systems and networks. This was seen in 2009, when cyber spies broke into the plans for the Pentagon’s Joint Strike Fighter project. Espionage is also a concern for Corporate America, where trade secrets are valuable, as economic cyber spies use similar techniques to their military counterparts to steal information from organizations.

Malicious Insiders

Disgruntled employees are a harmful brand of cybercriminal. For example, in July 2010, a couple was indicted for stealing and selling \$40 million worth of secret information related to General Motor’s hybrid plans to a Chinese automaker. The employee allegedly downloaded a confidential GM document and saved private GM information onto a hard drive. An

Please email the authors at fm pinguelo@nmmlaw.com or bwmuller@nmmlaw.com with questions about this article.

insider may also turn his technical prowess against his employer. In July 2010, a disgruntled database administrator received a year in prison for accessing and copying his ex-employer's customer database.

With insider cybercriminals being especially dangerous, employers must be proactive to protect their interests. One method is to watch historical patterns, which might help catch an employee who, for example, regularly accessed sensitive corporate information.

E-mail Extraction Programs and Spamming

Spamming involves sending unsolicited electronic mail to sell a product or collect data. These messages are sometimes used to deceive victims into sharing private information. In order to procure e-mail addresses for spamming, hackers have developed "e-mail extraction programs." In July 2010, a New Jersey man pleaded guilty to participating in a spam scheme that targeted universities. The conspirators utilized extraction programs to harvest millions of student e-mail addresses, which were then used for sending spam. As part of this effort, the men sent millions of e-mails through the University of Missouri's computer system.

Every employer should instruct its employees to take the following steps to help avoid some of spam's negative effects:

- Do not arbitrarily provide your business e-mail address to others, always report spam messages, and do not follow links provided in spam emails;
- Do not provide information about the organization, including its structure or networks, to outsiders; and
- If you believe you may have revealed private information about the organization's systems, report it to network administrators.

Hacking

Hackers sometimes crack into networks for profit, for sport, or for bragging rights. With attack tools becoming increasingly sophisticated and user-friendly, hacking remains a major concern. A recent example of hacking was seen in the BotNet Conspiracy. Allegedly, the conspirators created a program that could be used to hack into and control another person's computer. Once transmitted, the program caused the infected computers to log onto one of the conspirator's websites and wait for commands. With the "botnet" subject to their control, the men accessed

the user database of a website that offered web-hosting services. The database contained confidential user identifications and passwords, which the defendants downloaded. Soon thereafter, the men defaced the website and exposed the customers' user IDs and passwords.

Even some of our country's most popular websites are vulnerable to hacking, as seen in September 2010, when Twitter was hacked. One of the victims was the wife of former British Prime Minister Gordon Brown, as a link on her Twitter page sent visitors to a hard-core porn site.

Federal and State Action to Combat Cybercrime

Federal Executive Action

In January 2008, President Bush established the Comprehensive National Cybersecurity Initiative ("CNCI"). The goal of this program was to initiate a series of projects with a focus on reducing vulnerabilities, defending against intrusions, and preparing for future cyber threats. Cybersecurity remained in the spotlight when the Obama Administration took office. In February 2009, President Obama ordered a review of cybersecurity plans and programs, resulting in a May 2009 report which made recommendations for improving the nation's digital infrastructure. Despite these efforts, the executive branch fell victim to a successful cyber attack in July 2009, when a coordinated assault successfully disrupted the websites of several government agencies.

Federal Legislative Action

In February 2010, the House of Representatives passed H.R. 4061, the Cybersecurity Enhancement Act of 2010. The bill would assist the federal government's efforts to develop skilled personnel for its cybersecurity team, organize and prioritize the government's cybersecurity R&D, improve the shifting of cybersecurity technologies to the marketplace, and strengthen the role of the National Institute of Standards and Technology in developing cybersecurity public awareness and education programs.

The Senate's cybersecurity legislation, S.773, is currently stalled. According to recent reports, industry opposition and the mid-term elections make it unlikely that comprehensive reform will pass this year.

State Government Action: Virginia

Because Virginia is the home of America Online and several other Internet service providers, it has been dubbed "the epicenter of Internet traffic" and has

adopted some of the toughest cybercrime legislation in the country. Virginia's anti-spam legislation is a model for state government action.

The Virginia Computer Crimes Act includes, among other things, the Virginia anti-spam statute ("VAS"). The VAS criminalizes the use of "a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of spam through or into the computer network of an electronic mail service provider or its subscribers." A violation of this portion of the statute is a misdemeanor, but it may be upgraded to a felony if the amount of spam transmitted exceeds a certain amount or the revenue generated from the spam surpasses defined limits.

The statute also makes it a misdemeanor to knowingly sell, give, or otherwise distribute or possess with the intent to sell, give, or distribute software that

- (i) is primarily designed or produced for the purpose of facilitating or enabling the falsification of the transmission information or other routing information of spam; (ii) has only limited commercially significant purpose or use other than to facilitate or enable the falsification of the transmission information or other routing information of spam; or (iii) is marketed by that person acting alone or with another for use in facilitating or enabling the falsification of the transmission information or other routing information of spam.

As for enforcement, the Virginia Cyber Strike Force works with the U.S. Attorney's Office, State Police, and the FBI. With its comprehensive statutory and enforcement measures, Virginia is a model to other states.

Conclusion

Cybercrime is a societal problem that is difficult to combat. Nevertheless, we must take whatever steps possible to turn the tide against the growing hoard of cybercriminals. According to noted cyber law attorney Renato Opice Blum, "the reality is such that the profits from cybercrimes often surpass drug dealing, and the question now lies on which preventive and punitive measures should be taken. At a minimum, awareness and education are necessary to keep up with the pace of these criminals."