TRENDS IN CYBERCRIME:
THE DARK SIDE OF THE INTERNET

By Sean B. Hoar

It is part of the daily routine: You enter your office, turn on the computer, and click on the e-mail icon. This time you see three suspicious looking messages—two with attachments. One has an unfamiliar domain name and tells you to "PLEASE TREAT AS URGENT," the second is filled with digital gibberish, and the third appears to be from your brokerage company with a subject line that reads "Important Security Update."

The first time you were flooded with unsolicited e-mail, you naively opened a few out of curiosity and soon learned that at least one contained a hidden virus. It costs you thousands of dollars to have a forensic expert retrieve client data from the damaged hard drive, and a good measure of worry about what the thief might be doing with your confidential client information. But you also learned some valuable lessons. You learned that the simple act of opening an e-mail can download malicious software to your computer that allows someone to remotely monitor your key strokes, search for personal data on your hard drive, or implant a destructive virus. You also learned it is wise to delete messages from unfamiliar sources, and to install and update a firewall, antivirus protection, and a spam filter. You now provide your e-mail address to only those you trust and with whom you do business, and have even researched your ethical responsibilities to protect client data. But there seems to be no escape. It's now apparent that the scammers, spammers, and "phishers" have found you once again.

Cybercrime is so common that it is now part of our lexicon, defined as a crime committed on a computer network, especially the Internet. One of the fastest growing types of cybercrime, and perhaps most apparent to the typical computer user, is a form of online identity theft called "phishing" in which Internet users are spammed with official-looking e-mail messages in an attempt to persuade them to disclose personal information. Other forms of cybercrime include Internet fraud, computer intrusions (hacking), intellectual property theft, e-mail threats, online stalking, and child pornography.

So-called "social engineering" and/or malicious code are the two common methods used to commit cybercrime. Social engineering exploits relationships of trust, reduces situational awareness, or creates a sense of urgency. It assumes, for example, that some computer users are curious or trusting enough to open any e-mail message because they expect it to contain helpful information. Other victims willingly follow directives in an e-mail message where the sender appears familiar and the message creates a sense of urgency. Still others will act on the promises of rewards or merchandise and pay up-front, even when the sender is a stranger.

Malicious code, or "malware," is destructive software designed to damage, disrupt, alter, or steal data that comprise computer systems. Malware can be unwittingly downloaded when a victim opens an e-mail message, links to a Web site, or uses certain software (usually free, online downloads). The use of malware combined with social engineering can have devastating results.

Evolution of cybercrime

Development of the Internet began in 1969 by the Advanced Research Projects Agency of the U.S. Department of Defense. Known as ARPAnet, it was intended to be a fail-safe computer network that would continue to function even when other parts of the system failed. ARPAnet protocols were originally designed for transparency and flexibility—not security—in order to allow government and academic researchers to communicate with ease. (See *Security of the Internet*, 15 FROEHLICH/KENT ENCYCLOPEDIA OF TELECOMMUNICATIONS, 231-55 (Marcel Dekker, 1997).)

In 1986, the system recognized its first well-publicized security incident with an accidental discovery of an international effort to copy information from computers connected to ARPAnet. The covert intrusion alerted authorities to the destructive purposes to which ARPAnet could be put. Two years later, the first automated attack program, named for the Cornell student who wrote it, infected ARPAnet and replicated at such speed that it eventually shut down 10 percent of the 88,000 computers connected to the system. The Morris worm infected computers at leading universities, military sites, and medical research facilities, and caused an estimated $100 million in damages. (*See United States v. Morris*, 928 F.2d 504 (1991); *see also* Thomas M. Chen & Jean-Marc Robert, *Worm Epidemics in High-Speed Networks*, 37:6 COMPUTER, 48-53 (June 2004); and Paul A. Henry, *A Brief Look at the Evolution of Killer Worms*, CyberGuard Corporation, *at* http://www.cyberguard.com/news_room/white_papers/CG

_Killer_Worms.html?lang=de_EN (last visited Feb. 17, 2005).) The Morris worm prompted a number of organizations to form response entities to such threats, including what is now known as the Computer Emergency Response Team Coordination Center (CERT/CC), funded by the Defense Advanced Research Projects Agency.

By 1989, ARPAnet officially became the Internet and moved from a government research project to an operational network with more than 100,000 computers. Since then, the use of the Internet has experienced exponential growth. The *Computer Industry Almanac* estimates that there will be more than one billion Internet users by the end of 2005. (Computer Industry Almanac Inc., *Worldwide Internet Users Will Top 1 Billion in 2005* (Sept. 3, 2004) *available at* http://www.c-i-a.com/pr0904.htm).)

The growth of the Internet has been accompanied by an increase in newly detected system "vulnerabilities"—insecure areas that may threaten the security of a computer system. CERT/CC reports that newly detected vulnerabilities continue at an alarming pace with 1,220 reported in the first quarter of 2005—and these were on systems and applications previously perceived to be secure. This will break the previous record of 4,129 in 2002. (CERT Coordination Center, *CERT/CC Statistics 1988-2005* (last modified April 11, 2005) *at* http://www.cert.org/stats/cert_stats.html).

Exploitations of these vulnerabilities have exploded in the past few years, becoming household names: the Melissa worm in 1999, the Love Bug in 2000, the Code Red and the NIMDA worms in 2001. (See Chen & Robert, *Worm Epidemics in High-Speed Networks*; and Henry, *A Brief Look at the Evolution of Killer Worms.*) The number of new attacks upon Internet vulnerabilities has increased so greatly—from 21,756 in 2000 to 137,529 in 2003—and the incidents become so commonplace that CERT/CC no longer publishes the numbers. Unfortunately, the forces attacking the integrity of the Internet have succeeded so far in outmaneuvering those attempting to protect it.

On January 25, 2003, the SQL Slammer worm immediately shut down millions of computers. Overwhelmed with traffic, a critical transcontinental chain of routers began to fail. In Portugal, 300,000 cable modems shut down. In South Korea, 27 million were without cellular telephone or Internet service. Web sites throughout the Internet stopped responding. Emergency 911 dispatchers in Seattle resorted to paper. Unable to process tickets, Continental Airlines canceled flights from its Newark hub as most of its 75,000 servers were affected within the first 10 minutes. A variation of the SQL Slammer was reportedly responsible for a disruption at a nuclear power plant in Ohio on June 20, 2003. Another SQL Slammer variant was reported to be at least partially responsible for the August 14, 2003, power failure that blacked out cities from Ohio to New York. It is estimated that the SQL Slammer cost $1.2 billion. (See GAO, *Information Security—Effective Patch Management Is Critical to Mitigating Software Vulnerabilities*, GAO-03-1138T (Sept. 10, 2003); and Henry, *A Brief Look at the Evolution of Killer Worms.*)

In 2004, nearly 115 million computers were infected by 480 new species of malicious code, including the worms MyDoom, NetSky, SoBig, Klez, and Sasser, which cost at least $166 billion. (*2004: Year of the global malware epidemic—Top ten lessons*, IT OBSERVER (Nov. 23, 2004) *at* at http://www.ebcvg.com/press.php?id=679). Almost 50 percent of this malicious code was designed to obtain confidential information. (*Symantec Internet Security Threat Report Highlights Rise in Threats to Confidential Information*, (March 21, 2005) *at* http://www.symantec.com/press/2005/n050321). In 2005, the dissemination of new malicious code continues at an exponential rate. (*The number of new viruses detected has increased 278% since the third quarter of 2004, Panda Software reports*, (April 25, 2005) *at* http://www.pandasoftware.com/about/press/viewNews.aspx?noticia=6146). Most of the new code appears driven toward profit rather than destruction. (*Q2 Virus Roundup: Outbreak Incidents and Prevailing Malware Trends* (last visited Aug. 5, 2005) *at* http://www.trendmicro.com/NR/rdonlyres/1D333BB8-55BA-4A92-94AFD6C8E4A5F3ED/16469/Q22005Roundup.pdf). Over the years, immeasurable data have been stolen from sensitive government sites including NASA and the Departments of Defense and Energy, and billions of dollars of proprietary information has been stolen from private sites. In February 2003, in response to the obvious vulnerability of the Internet, the White House released the *National Strategy to Secure Cyberspace*. The first paragraph of the executive summary aptly described the critical role of the Internet:

> Our Nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their

---

Sean B. Hoar *has served with the United States Department of Justice in Eugene, Oregon, as an assistant United States attorney since 1991. He coordinates training for law enforcement officers and prosecutors on the investigation and prosecution of identity theft and Internet fraud, and on search and seizure laws pertaining to electronic evidence. He is a member of a national network of assistant United States attorneys who provide legal assistance in computer-crime emergencies, and he teaches a course in cybercrime at the University of Oregon School of Law.*

> nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security.

(*The National Strategy to Secure Cyberspace* (Feb. 2003), http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf).

The 60-page document recognized that our economy and national security are dependent upon the Internet, the core of our information technology and the information infrastructure. This infrastructure controls everything from electrical grids to stock markets. The objectives of the national strategy are to prevent cyberattacks against America's critical infrastructures, reduce national vulnerability to cyberattacks, and minimize damage and recovery time from cyberattacks that do occur. The critical priorities to be achieved are (1) the development of a national cyberspace security response system, (2) the development of a national cyberspace security threat and vulnerability reduction program, (3) the development of a national cyberspace security awareness and training program, (4) securing the cyberspace of local, state, and federal government, and (5) strengthening national security and international cyberspace security cooperation.

Unfortunately, even as the vulnerability of our critical infrastructures increases, little has been done to implement the national strategy. This inaction prompted the Cyber Security Industry Alliance (CSIA) to urge President Bush in his second term to exert leadership to implement the plan. The CSIA proposed a federal agenda that (1) raises the profile of cybersecurity, (2) promotes information sharing, threat analysis, and contingency planning, and (3) boosts the efforts in research and development, and security education. (Cyber Security Industry Alliance, *Agenda for the Next Administration* (Dec. 7, 2004), http://www.csialliance.org/resources/pdfs/Agenda_for_Next_Administration.pdf).

Although the original architecture of the Internet was appropriate for its initial purposes, it lacks the necessary integrity for secure commerce and communication. Even with the assistance and scrutiny of industry experts, and billions of dollars spent over the years on the development of less vulnerable operating systems and secure software applications, security problems have continued. Opportunities for cybercrime abound.

The crime: Online identity theft

Just a few years ago, online identity theft was seen as a relatively small aspect of the larger identity theft problem; but today, due to its ease and lucrative results, online identity theft is the fastest growing type of cybercrime. Its insidious nature is defined by the anonymity afforded the perpetrators and the devastating impact it has on its victims, compounded by the fact that the economic harm often is not discovered until long after the crime has occurred and the thieves have disappeared.

Due to recently enacted data breach disclosure laws, consumers have begun to learn the scope of the online identity theft problem. One of the first public disclosures of a data breach occurred on February 14, 2005, after identity thieves accessed personal information of more than 145,000 consumers contained in databases compiled by ChoicePoint in Atlanta, Georgia. (Bob Sullivan, *Database giant gives access to fake firms*, MSNBC.Com (Feb. 14, 2005) at http://www.msnbc.msn.com/id/6969799/). Unfortunately, this was only a "minor" breach when compared to several subsequently reported incidents. Perhaps the most infamous was disclosed on June 16, 2005, after identity thieves exploited vulnerabilities in databases compiled by CardSystems Solutions Inc. in Tucson, Arizona, accessing personal information of more than 40 million consumers. (Kim Zetter, *CardSystem's Data Left Unsecured*, Wired.Com (Jun. 22, 2005) at http://www.wired.com/news/technology/0,1282,67980,00.html). Between March 8 and July 30, 2005, intrusions into electronic databases in the United States through Internet vulnerabilities caused more than 42 million consumers to become victims of identity theft. (*A Chronology of Data Breaches Reported Since the ChoicePoint Incident*, Privacy Rights Clearinghouse (updated July 30, 2005) *at* http://www.privacyrights.org/ar/ChronDataBreaches.htm).

"Phishing," the act of sending a bogus e-mail to an unsuspecting user that appears to be from a legitimate enterprise, is a common method of identity theft. It is employed by thieves who hope to persuade a user to provide personal information that will allow them to assume the victim's identity. Phishing, as with its real-world counterpart, allows Internet scammers to use e-mails as lures to "fish" for credit card account numbers, Social Security numbers, online passwords, and other personal data. Also called "brand spoofing" or "carding," phishing relies on the fact that while most Internet users will ignore the bait, there will always be a few who can be tempted to bite. (Anti-Phishing Working Group, *Origins of the Word "Phishing*" (last visited Aug. 5, 2005) http://www.antiphishing.org/word_phish.html).

According to one study, phishing caused approximately $1.2 billion in direct losses to banks and credit card issuers in the United States in 2003. It went on to report that 30 million adult Internet users believed they had recently experienced a phishing attack, while another 27 million suspected they had witnessed a phishing attack. Unfortunately, such phishing expeditions appear to have a high rate of success. About 19 percent of those attacked, or nearly 11 million adult Internet users in the United States, clicked on the links in the bogus e-mail, and 3 percent of those—an estimated 1.78 million adults—said

they had given phishers their financial or personal information. (GARTNER, *Gartner Study Finds Significant Increase in E-Mail Phishing Attacks* (May 6, 2004) http://www4.gartner.com/press_releases/asset_71087_11.html).

According to the Anti-Phishing Working Group (APWG) such attacks continued to rise sharply in 2005 with the use of "unique" phishing e-mail in which a single e-mail with a unique subject line is "blasted" at a targeted company or organization. In June 2005, APWG received reports of 15,050 unique phishing messages—compared to 8,829 in December 2004. APWG also reported the use of increasingly sophisticated malicious code to obtain confidential information. (Anti-Phishing Working Group, *Phishing Activity Trends Report, June 2005* (last modified Aug. 3, 2005) http://www.antiphishing.org/index.html).

Phishing takes on a variety of guises. It may involve using an e-mail format that mimics that of a legitimate organization in order to deceive one of its customers, or it may involve the falsification of industries that purportedly exists to mitigate risks, such as escrow or financial intermediaries.

The most dangerous form, however, is malicious software. Also called "malware," it is downloaded to an unsuspecting victim's computer when the user opens an e-mail message, an attachment, or clicks on a hyperlink within a bogus message. It may then disseminate viruses and/or worms designed to harvest the user's private information. Malware may also insert key-logger programs that allow the phisher to remotely record the victim's key strokes in order to capture credit card account, bank account, or password information, or it may insert remote screen capture applications. Malware may also be downloaded via peer-to-peer file sharing programs or from pirated software.

Until recently, the financial industry considered losses from online crime as the "cost of doing business." But the $1.2 billion in losses and damage done to the industry's reputation have banks and credit card issuers changing their practices. Ironically, it is the very success of the phishers that has led financial institutions and the government to more urgently pursue a cleanup of the Internet. Online identity theft has led to the creation of associations, alliances, working groups, and initiatives involving the largest banks, Internet service providers, technology vendors, and law enforcement entities. (*See*, *e.g.*, Anti-Fraud Alliance, *Industry-Leading Security Solution Providers Form Anti-Fraud Alliance* (Nov. 17, 2004) *at* http://www.antifraudalliance.com/html/release.html). As one anti-phishing Web site recently stated: "Phishing is about to become a very dangerous sport." (Digital Phishnet *at* http://www.digitalphishnet.org).

Applicable federal laws

Identity theft. Title 18 U.S.C. § 1028(a)(1)-(8) proscribes eight different types of document and identification fraud. Section 1028(a)(7) is the primary federal identity theft statute, and is the most applicable subsection to online identity theft. It prohibits anyone, under certain circumstances giving rise to federal jurisdiction, from knowingly transferring, possessing or using, without lawful authority, a "means of identification" of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law. (18 U.S.C. § 1028(a)(7).) The jurisdictional component requires that the transfer, possession, or use of the means of identification occur in or affect interstate or foreign commerce, or involve the mail. (18 U.S.C. § 1028(c)(3).) The term "means of identification" refers to any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual. (18 U.S.C. § 1028(d)(7).) Note that the federal, state, or local law that is facilitated by the identity theft must also be proven. The statutory maximum penalties range from up to five to 25 years in prison, depending upon the facts pled and proven. (18 U.S.C. § 1028(b).)

Aggravated identity theft. On July 15, 2004, the Identity Theft Penalty Enhancement Act was signed into law. Among other things, it creates a new offense of aggravated identity theft, which prohibits the knowing and unlawful transfer, possession, or use of a means of identification of another person during and in relation to any of more than 100 felony offenses (including section 1028 offenses other than 1028(a)(7)). (18 U.S.C. § 1028A(a)(1), (c).) These offenses include those commonly associated with identity theft such as mail, bank, and wire fraud, immigration and passport fraud, and any unlawful use of a Social Security number. (18 U.S.C. § 1028A(c).) Note that the felony committed during and in relation to the identity theft must also be proven. Aggravated identity theft is punishable by a minimum mandatory two years in prison consecutive to the sentence for the underlying felony. (18 U.S.C. § 1028A(a)(1).) If the offense is committed during and in relation to one of more than 40 federal terrorism-related felonies, the penalty is a minimum mandatory five years in prison consecutive to the sentence for the underlying felony. (18 U.S.C. § 1028A(a)(2).)

Federal prosecutors are required to file the most serious, readily provable offense supported by the facts. The most serious offense is the one for which a defendant will receive the longest sentence under the sentencing guidelines. (Memorandum from Attorney General John Ashcroft to all federal prosecutors regarding department policy concerning charging criminal offenses, disposition of charges, sentencing (Sept. 22, 2003) *at*

http://www.usdoj.gov/opa/pr/2003/September/03_ag_516.htm). In most federal identity theft cases, such as the unlawful use of a Social Security number to commit bank fraud, a violation of section 1028(a)(7) will also constitute a violation of section 1028A. This means that in most federal identity theft offenses committed subsequent to July 15, 2004, federal prosecutors will be required to charge aggravated identity theft under section 1028A and subject offenders to a minimum mandatory sentence consecutive to the underlying guideline sentence.

Bank fraud. Online identity theft often facilitates bank fraud. The acquisition of a Social Security number is the master key to identity theft. The Social Security number is frequently the only means of identification used to verify credit, and is often not cross-referenced to the actual name and date of birth of the person to whom the number was assigned. Identity thieves are, therefore, often able to open bank accounts with fictitious names while using someone else's Social Security number. Title 18 U.S.C. § 1344 prohibits anyone from knowingly executing or attempting to execute a scheme to defraud a financial institution, or to obtain money or property owned by or under the custody or control of a financial institution by means of false representations. It is punishable by up to a $1 million fine and 30 years in prison. (18 U.S.C. §§ 1343, 3571(b)(1).)

Credit card fraud. Online identity theft also facilitates credit card fraud. Title 18 U.S.C. § 1029(a)(1)-(10) proscribes 10 types of "access device" fraud. An "access device" is essentially any means of account access, such as a credit card, that can be used alone or in conjunction with another access device to obtain something of value. (18 U.S.C. § 1029(e)(1).) Online identity theft frequently involves violations of section 1029(a)(1) or (2). Section 1029(a)(1) prohibits anyone from knowingly and with intent to defraud, producing, using, or trafficking in one or more counterfeit access devices. Section 1029(a)(2) prohibits anyone from knowingly and with intent to defraud, trafficking in or use one or more unauthorized access devices during any one-year period, and thereby obtaining anything of value aggregating $1,000 or more during that period. It is punishable by up to 10 to 20 years in prison, depending upon the facts pled and proven. (18 U.S.C. §§ 1029(c).)

The crime: Internet fraud

The term "Internet fraud" refers generally to any type of fraud occurring online. The various types of Internet fraud parallel those committed offline. The destructive effect of Internet fraud, however, is compounded due to the ease and anonymity with which it can be committed, and the immediate access the Internet provides to a huge number of potential victims. Internet fraud harms not only consumers, but undermines their confidence in legitimate e-commerce and the Internet, thereby harming business concerns. It is estimated that online fraud cost electronic commerce Web sites $2.6 billion in 2004—an increase of $700 million over 2003. (Bob Sullivan, *Online Fraud Costs $2.6 Billion This Year*, MSNBC.Com (Nov. 11, 2004) *at* http://www.msnbc.msn.com/id/6463545; *Ecommerce Fraud Losses to Jump $700 Million in 2004*, CYBERSOURCE (Nov. 15, 2004) *at* http://www.cybersource.com/news_and_events/view.xml?page_id=1313).

In 2003 and 2004, three major law enforcement initiatives targeted Internet fraud: Operation E-Con, Operation Cyber Sweep, and Operation Web Snare. The most common Internet fraud schemes uncovered involved advance fee fraud, business/employment fraud, counterfeit check fraud, credit/debit card fraud, freight forwarding/reshipping fraud, identity theft, investment fraud, nondelivery of goods/services, auction/retail fraud, phony escrow services, and ponzi/pyramid schemes. (Internet Crime Complaint Center, *IC3 2003 Internet Fraud Report*, pp. 25-28 http://www.ifccfbi.gov/strategy/2003_IC3Report.pdf). Each of the initiatives was coordinated at the federal level through the Fraud Section of the United States Department of Justice, in association with the FBI, the Internet Crime Complaint Center (ICC), the U.S. Postal Inspection Service, the U.S. Secret Service, the FTC, the Bureau of Immigration and Customs Enforcement, numerous state and local law enforcement agencies, and a number of private industry partners. The National White Collar Crime Center (NWCC) contributed significantly in coordinating state and local law enforcement agencies.

Operation E-Con involved more than 90 investigations, 89,000 victims, $176 million in estimated losses, and more than 130 convictions. (U.S. Dep't Just., *Justice Department Announces Dozens of Arrests in Nationwide Internet Fraud Takedown, Operation E-Con*, (May 16, 2003) http://www.usdoj.gov/opa/pr/2003/May/03_crm_301.htm). Operation Cyber Sweep involved more than 125 investigations, 125,000 victims, $100 million in estimated losses, and more than 125 convictions. (U.S. Dep't Just., *Justice Department Announces "Operation Cyber Sweep" Targeting Online Economic Fraud* (Nov. 20, 2003) *at* http://www.fbi.gov/dojpressrel/pressrel03/cyber112003.htm). Operation Web Snare involved more than 160 investigations, 150,000 victims, $215 million in estimated losses, and more than 150 convictions. (U.S. Dep't Just., *Justice Department Announces Operation Web Snare Targeting Online Fraud and Crime* (Aug. 26, 2004) *at* http://www.usdoj.gov/opa/pr/2004/August/04_crm_583.htm).

Applicable federal laws

Wire (Internet) fraud. Title 18 U.S.C. § 1343 prohibits anyone from transmitting, by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing a scheme to defraud. It is punishable by a $250,000 fine and 20 years in prison. If the

offense affects a financial institution it is punishable by a fine of up to $1 million and 30 years in prison. (18 U.S.C. §§ 1343, 3571(b)(1) and (3).)

Mail fraud. Internet fraud usually involves mail fraud, to the extent the mail is used to facilitate the fraud or to receive anything obtained by fraud. Title 18 U.S.C. § 1341 prohibits anyone from using the mail, including a private or commercial mail carrier, for the purpose of executing a scheme to defraud. It is punishable by a $250,000 fine and 20 years in prison. If the offense affects a financial institution it is punishable by a fine of up to $1 million and 30 years in prison. (18 U.S.C. §§ 1341, 3571(b)(1) and (3).)

Internet fraud also commonly involves violations of bank fraud, credit card fraud, and identity theft.

The crime: Computer intrusion

The term "computer intrusion," or "hacking," refers to unauthorized access to a computer or other digital processing or storage device. "Hacking" harks back to the 1960s when student members of MIT's Tech Model Railroad Club "hacked" switches and control systems of electric trains to increase their performance. They then transferred their curiosity to MIT's new mainframe computer system. (M. Mitchell Waldrop, THE DREAM MACHINE: J.C.R. LICKLIDER AND THE REVOLUTION THAT MADE COMPUTING PERSONAL, 187-88 (2002).) Hacking has since become malicious and automated, costing an estimated $166 billion in 2004. (*2004: Year of the global malware epidemic—Top ten lessons*, IT OBSERVER (Nov. 23, 2004) *at* http://www.ebcvg.com/press.php?id=679).

Automated attacks are so prevalent that Postini, a provider of e-mail security and management to businesses, reported that 88 percent of the 6.9 billion e-mail messages it processed in November of 2004 were spam, viruses, phishing attacks, or directory harvest attacks (in which the spammer tries to hijack an organization's entire e-mail directory in order to send spam to other corporate e-mail servers). Only 12 percent of the messages were legitimate. (Postini, *Postini Reports That Only 12% of All E-mail Messages Were Legitimate During the Month of November* (Dec. 1, 2004) http://www.postini.com/news_events/pr/pr120104.php).

Two private surveys, one in cooperation with the U.S. Secret Service and CERT/CC, and another in cooperation with the FBI Computer Intrusion Squad in San Francisco, recently found that viruses or other malicious code were the most cited form of attack (more than 80 percent). The system attacks included virus or other malicious attacks, unauthorized access to information, denial of service attacks, abuse of wireless networks, theft of proprietary information, sabotage, financial fraud, and Web site defacements. (CSO MAGAZINE, *2005 E-Crime Watch Survey—Survey Results* (July 1, 2005), http://www.csoonline.com/info/ecrimesurvey05.pdf; Computer

NATIONAL STRATEGY TO SECURE CYBERSPACE

In February 2003, the White House released the National Strategy to Secure Cyberspace. The first paragraph of the executive summary aptly described the critical role of the Internet in our society:

> Our Nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security.

(*The National Strategy to Secure Cyberspace* (Feb. 2003) http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf).

The 60-page document lists the government's strategic objectives: to prevent cyberattacks against America's critical infrastructures, reduce national vulnerability to cyberattacks, and minimize damage and recovery time from those cyberattacks that do occur. The critical priorities are (1) the development of a national cyberspace security response system, (2) the development of a national cyberspace security threat and vulnerability reduction program, (3) the development of a national cyberspace security awareness and training program, (4) securing the cyberspace of local, state, and federal government, and (5) strengthening national and international cyberspace security cooperation.

Security Institute, *2005 CSI/FBI Computer Crime and Security Survey*, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf).

Cellular telephones are the latest targets for such attacks. The first worms capable of attacking cell phones were detected in 2004. Indications are that these attacks could prove even more prolific than those against personal computers (PCs) because there are so many more cell phones than PCs, and cell phone vendors opened their operating platforms to third parties in order to develop Internet accessible applications. Also, cell phones are utilized to conduct both conversation and commerce, making them a hacker's dream: millions of Internet-enabled electronic devices with sophisticated banking functions and open interfaces. (See John Blau, *Mobile phones: An ear full of worms*, COMPUTERWORLD (Dec. 8, 2004) http://www.computerworld.com/mobiletopics/mobile/story/0,10801,98123,00.html).

The proliferation of spam. The first conviction under the CAN-SPAM Act of 2003 occurred in September 2004 when Nicholas Tombros pled guilty to using a laptop computer in his car to access wireless Internet accounts and send e-mail advertising pornographic Web sites. In pleading guilty, Tombros admitted that he went "war-driving" in the California community of Venice Beach looking for unprotected wireless access points from which to spam numerous victims with e-mail advertising pornographic Web sites. (U.S. Dep't of Just., *Guilty plea by local "War-Spammer" is first-ever conviction under CAN-SPAM Act* (Sept. 28, 2004) http://www.usdoj.gov/usao/cac/pr2004/131.html).

Old-fashioned hacking continues to occur as well. In December 2004, Gregory Herns of Portland, Oregon, was sentenced to serve six months in federal prison for hacking into the NASA's Goddard Space Flight Center, ostensibly to store movies he had downloaded. The intrusion caused systems to crash and cost NASA more than $200,000. (Noelle Crombie, *Local hacker who hit NASA gets 6 months*, OREGONIAN (Dec. 18, 2004) http://www.oregonlive.com/news/oregonian/index.ssf?/base/front_page/1103374759206520.xm).

Applicable federal laws

Computer fraud and abuse. Title 18 U.S.C. § 1030(a) prohibits:

1. accessing a computer without authorization and obtaining information pertaining to national security, *see id*. § 1030(a)(1);

2. accessing a computer without authorization and obtaining information pertaining to certain consumer financial information, information from a federal agency, or information from any other protected computer, *see id*. § 1030(a)(2) (a protected computer means, among other things, that the computer is used in interstate commerce, *see* 18 U.S.C. § 1030(e)(2));

3. the intentional but unauthorized access to a government computer, *see id*. § 1030(a)(3);

4. the unauthorized access to a protected computer with the intent to defraud, unless the object of the fraud or anything obtained consists only of the use of the computer and is not more than $5,000 in any one-year period, *see id*. 1030(a)(4);

5. trafficking in passwords, *see id*. § 1030(a)(6); and

6. the transmission of any threat to cause damage to a computer used in interstate commerce with the intent to extort anything of value, *see id*. § 1030(a)(7).

Section 1030(a)(5) is the traditional hacking statute. Section 1030(a)(5)(A)(i) prohibits the knowing transmission of code that intentionally causes damage to a protected computer. Section 1030(a)(5)(A)(ii) prohibits the intentional access to a protected computer that recklessly causes damage. Section 1030(a)(5)(A)(iii) prohibits the intentional access to a protected computer that negligently or accidentally causes damage. Each of the section 1030(a)(5)(A) offenses must also satisfy at least one of five other conditions. These conditions include causing a loss of at least $5,000, or causing damage to a computer used by a government entity in the administration of justice, national defense, or national security. (18 U.S.C. § 1030(a)(5)(B)(i) and (v).) Damage means any impairment to the integrity or availability of data. (18 U.S.C. § 1030(e)(8).) Penalties for these offenses range from up to one year to life in prison, depending upon the facts pled and proven. (18 U.S.C. § 1030(c).)

Spam. The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) proscribes five types of conduct associated with the dissemination of e-mail. (18 U.S.C. § 1037(a)(1)-(5).) This type of conduct may involve Internet fraud, but is often a form of unauthorized access to computer systems. Section 1037(a)(1) prohibits hacking in order to spam. It proscribes the intentional transmission of multiple commercial electronic mail messages from a protected computer without authorization. The term "multiple" means more than 100 e-mail messages during a 24-hour period, more than 1,000 e-mail messages during a 30-day period, or more than 10,000 e-mail messages during a one-year period. (18 U.S.C. § 1037(d)(3).)

Section 1037(a)(2) prohibits using a relay to deceive. It proscribes the use of a protected computer to relay multiple commercial electronic mail messages with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of the messages. Section 1037(a)(3) prohibits the use of false header information. It proscribes the intentional transmission of multiple commercial electronic mail messages containing materially false header information. Section 1037(a)(4) prohibits anonymous e-mail abuse. It proscribes the transmission of multiple commercial electronic mail messages from five or more

electronic mail accounts or online user accounts or two or more domain names that were registered with false information. Section 1037(a)(5) prohibits "zombie spam," or the intentional transmission of multiple commercial electronic mail messages from five or more Internet protocol addresses falsely represented to be that of the sender. Penalties for these offenses range from up to one year to five years in prison, depending upon the facts pled and proven. (18 U.S.C. §§ 1037(b).)

The crime: Intellectual property offenses

Intellectual property theft costs U.S. companies and estimated $250 billion annually. (U.S. Dep't of Just., *Report of the Department of Justice's Task Force on Intellectual Property* (October 2004) p. 8, *at* http://www.cybercrime.gov/IPTaskForceReport.pdf). Intellectual property is defined by the four areas of the law that protect it: copyrights, trademarks, trade secrets, and patents. Copyright law provides federal protection against infringement of certain exclusive rights, such as reproduction and distribution, of original works of authorship, including computer software, literary works, musical works, and motion pictures. The use of a commercial brand to identify a product is protected by trademark law, which prohibits the unauthorized use of any word, name, symbol, or device used by a person to identify and distinguish goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods. Trade secret law provides legal protection for any formula, device, or compilation of information used in a business from being disclosed without the owner's permission. Legal protection is only afforded to those trade secrets that possess independent economic value and which the owner has taken reasonable measures to keep secret.

Applicable federal laws

Criminal copyright infringement. Title 18 U.S.C. § 2319(a) and 17 U.S.C. § 506(a) prohibit the reproduction or distribution of copyrighted works, such as software programs and musical recordings, even if the defendant acts without a commercial purpose or for private financial gain. If the offense involves the reproduction or distribution of 10 or more copyrighted works having a total retail value of more than $2,500 during any 180-day period, and the defendant acts for purposes of commercial advantage or private financial gain, it is punishable by up to five years in prison and a $250,000 fine. If the offense involves the reproduction or distribution of 10 or more copyrighted works having a total retail value of more than $2,500 during any 180-day period, but is not committed for purposes of commercial advantage or private financial gain, it is punishable by up to three years in prison and a $250,000 fine. If the offense involves the reproduction or distribution of one or more copies of copyrighted works with a value of more than $1,000, it is punishable by up to one year in jail and a $100,000 fine.

Counterfeit trademarks. The Trademark Counterfeiting Act, 18 U.S.C. § 2320(a), prohibits the intentional trafficking or attempt to traffic in goods or services while knowingly using a counterfeit mark on or in connection with the goods or services. It is punishable by up to 10 years in prison and a $2 million fine.

Counterfeit labeling. Title 18 U.S.C. § 2318 prohibits trafficking in counterfeit labels designed to be affixed to copies of computer programs, motion pictures, and audiovisual works, as well as trafficking in counterfeit documentation or packaging for computer programs. It is punishable by up to five years in prison and a $250,000 fine.

Theft of trade secrets. The Economic Espionage Act contains two separate provisions that criminalize the theft of trade secrets. The first provision, 18 U.S.C. § 1831(a), prohibits thefts of trade secrets for the benefit of a foreign government or agent, and is punishable by up to 15 years in prison and a $500,000 fine. The second, 18 U.S.C. § 1832, prohibits thefts of commercial trade secrets, and is punishable by up to 10 years in prison and a $250,000 fine. The statute broadly defines the term "trade secret" to include all types of information that the owner has taken reasonable measures to keep secret and that has independent economic value.

The crime: Child pornography

It is estimated that child pornography, which generates $3 billion annually, is requested 116,000 times daily through certain peer-to-peer file sharing programs, and is featured on more than 100,000 Web sites. Victimizing the most innocent in society, sexual predators now exploit children, from toddlers to teens, not only for their own gratification, but for all those who choose to view these photos and films via the Internet. In addition, it is estimated that one in five children old enough to use the Internet receive online sexual solicitations. (Internet Filter Review, *Internet Pornography Statistics* (visited December 10, 2004) http://www.internetfilterreview.com/internet-pornography-statistics.html; Family Safe Media, *Pornography Statistics 2003* (visited December 10, 2004) http://www.family safemedia.com/pornography_statistics.html).

Child pornography cases are often made when FBI agents pose as participants in Internet user groups or chat rooms where pornographic photos and videos have been posted. Individuals from all walks of life participate in the distribution of child pornography. (See TeCrime International, Inc., *Online pornography and child pornography cases by state* (visited December 10, 2004) http://www.tecrime.com/llartpST.htm). In May 2003, the Rev. Thomas James, of Vancouver, Washington, used an online chat room to arrange a meeting with a 13-year-old girl in a parking lot of a convenience store in Portland,

Oregon. But his intended victim turned out to be an FBI agent, and James later pled guilty to traveling across state lines with the intention of engaging in sex with a minor. (Mark Larabee, *Minister pleads guilty in online sex case*, OREGONIAN (Oct. 7, 2003) http://www.tecrime.com/llartL27.htm).

Applicable federal laws

Possession, manufacture, or distribution of child pornography. Title 18 U.S.C. § 2252A prohibits, among other things, the knowing distribution, receipt, or possession of any visual depiction of a minor engaging in sexually explicit conduct. The statutory minimum penalties range from five to 15 years in prison, and the statutory maximum penalties range from 10 to 40 years in prison, depending upon the facts pled and proven.

Using the Internet to entice sexual activity. Title 18 U.S.C. § 2422(b) prohibits anyone to knowingly use a facility of interstate commerce (the Internet) to persuade, induce, entice, or coerce a minor to engage in criminal sexual activity. The statutory penalty is five to 30 years in prison.

Traveling in interstate commerce with the intent to engage in criminal sexual activity. Title 18 U.S.C. § 2423(b) prohibits anyone to knowingly travel in interstate commerce with the intent to engage in criminal sexual activity with a minor. It is punishable by up to 30 years in prison.

The crime: Material support for terrorists

The Internet has become the new Afghanistan for terrorist training, recruitment, and fund-raising. Terrorist groups are exploiting the accessibility, vast audience, and anonymity of the Internet to raise money and recruit new members. (See Aaron Aft, *Terror Groups Exploit Internet for Communications, Recruiting, Training*, The Jewish Institute for National Security Affairs (Aug. 4, 2004) *available at* http://www.jinsa.org/articles/articles.html/function/view/categoryid/1930/documentid/2621/history/3,2359,2166,1930,2621). There are reportedly more than 4,000 Web sites associated with terrorist organizations. According to the Middle East Media Research Institute, many are hosted in the United States. (See Marie-Helene Boccara, *Islamist Websites and Their Hosts Part I: Islamist Terrorist Organizations*, The Middle East Media Research Institute (July 16, 2004) *available at* http://www.memri.org/bin/articles.cgi?Page=archives&Area=sr&ID=SR3104).

Applicable federal law

Title 18, U.S.C. § 2339A, prohibits anyone from providing "material support or resources" to anyone knowing it will be used to commit one or more terrorist-related offenses. The term "material support or resources" means financial support, training, expert advice, or assistance—with the exception of medicine or religious materials. (18 U.S.C. § 2339A(b).) The statutory penalties range from 15 years to life in prison, depending upon the facts pled and proven.

Jurisdictional issues

Jurisdictional borders pose unique challenges to the investigation of crimes committed in cyberspace. In most Internet fraud cases, the perpetrators reside in a jurisdiction other than that of their victims. In order to investigate such a case, evidence must be obtained from multiple jurisdictions. Many state law enforcement authorities, however, are precluded from issuing legal process to obtain evidence outside their jurisdiction. This impediment often precludes pursuit of the offender. In addition to more than 87,000 local jurisdictions, there are more than 3,000 county jurisdictions, 50 state jurisdictions, and 94 federal jurisdictions in the United States. Given the jurisdictional obstacles, law enforcement authorities in all jurisdictions must work together to pursue offenders, collect evidence, and assist victims of cybercrime.

International issues

The Internet has no geographical or political boundaries, and can be accessed from anywhere in the world. The perpetrators of cybercrime regularly use this to their advantage. The global reach of the Internet requires that a transnational legal framework be developed to allow and encourage international cooperation in the investigation and prosecution of cybercrime. On November 23, 2001, in Budapest, Hungary, a step was taken toward that goal when the United States and 29 other countries signed the Council of Europe Cybercrime Convention. It is the first multilateral treaty to specifically address computer-related crime and electronic evidence gathering.

The Cybercrime Convention will accomplish three major objectives. First, each member country is to enforce certain laws, including those against intentional and serious computer hacking, illegal interception, forgery, fraud, child pornography, and intellectual property infringement. (Articles 2-11.) Second, each member country is to adopt basic national legal procedures, investigatory tools, and human rights safeguards that most nations, including the United States, already have in their legal systems. (Articles 16-22.) Third, it encourages international cooperation in the investigation and prosecution of cybercrime. (Articles 23-35.) The treaty must be ratified by the president of the United States after receiving the advice and consent of the U.S. Senate. President Bush sent the document to the Senate on November 17, 2003, but other than a hearing by the Senate Foreign Relations Committee on June 17, 2004, no further action has been taken by the Senate. Unfortunately, until investigators and prosecutors can count on immediate

and reliable international cooperation, countless offenders will continue to victimize with impunity.

Conclusion and recommendation

Our economy and national security are dependent upon the Internet, and will continue to be adversely impacted by cybercime. As long as the Internet remains vulnerable to malicious code, profitable opportunities for cybercrime will continue to increase. As long as profitable opportunities for cybercrime exist, cybercrime will threaten our privacy and prosperity. It is imperative that we invest the resources to increase the security of computer systems that comprise the Internet. It requires individual and organizational responsibility. It also requires cooperation and resources from both government and private industry.

In order to reduce the vulnerability of the Internet, the strategic objectives set forth in the National Strategy to Secure Cyberspace—the prevention of cyberattacks against our critical infrastructures, the reduction of national vulnerability to cyberattacks, and the minimization of damage and recovery time from cyberattacks that do occur—must be implemented. Until these objectives are accomplished, cybercrime will continue to wreak havoc on the economy in direct monetary losses, productivity losses, and the theft of identities and intellectual property. Cybercrime will also continue to increase the risk of catastrophic system failure by weakening our critical infrastructure. The good news is that there exist tremendous intellectual and technological resources to meet the challenge. With leadership and persistent effort, we can turn the tide on cybercrime.■