



CORPORATE HOMICIDE™

LIFE IN A GLOBAL ECONOMY

A NEWSLETTER FOR THE SECURITY AND NON-SECURITY EXECUTIVE

The Sting - - - A Los Angeles jury found Patrick Naughton, a key member of the team that created Sun Microsystems Inc.'s Java computer programming language and more recently oversaw the Go Network of Web sites created by Infoseek and Walt Disney, guilty of possessing child pornography. The jury failed to reach a verdict on two other felony charges that Naughton used the Internet and crossed state lines to have sex with a minor. **Naughton pleaded not guilty to all three federal charges**, claiming that his "dirty talk" with a girl identifying herself as being 13 years old was just fantasy. **The "girl" was in fact an FBI agent**. By trolling the Net disguised as young girls and boys, FBI agents have arrested more than 700 people on charges of trafficking in child pornography or luring minors across state lines for sexual encounters, according to the bureau. The **FBI's Innocent Images program**, which focuses on these crimes, has received \$10 million in funding in the last two years. **As these local and federal Net stings proliferate, civil liberties groups and defense attorneys** are closely monitoring the operations, and some convictions are being challenged on constitutional grounds. "The potential problems range from entrapment to illegal search and seizures," said American Civil liberties staff attorney Ann Beeson.

Entrapment - - - Naughton was charged with interstate travel with the intention of having sex with a minor. Aside from the possible claim of entrapment, which is extremely difficult to prove, the arrest doesn't raise a host of constitutional issues, according to legal experts. **"The principle behind entrapment is that the government may not try to persuade someone to commit a crime who wouldn't otherwise do it,"** said Eugene Volokh, a law professor at the University of California at Los Angeles.

Defense - - - Suspects arrested in California have been charged under a state penal code that targets sexually explicit communication with minors over the Net. The statute prohibits using e-mail or the Net to "knowingly" expose minors to any "harmful" matter with the intent of seducing, arousing, or sexually gratifying them. **The California law firm of Clancy, Weisinger & Associates is defending a handful of clients charged under the act**. The firm's attorneys argue that the law is unconstitutional because it is impossible to establish the age of a Net user. In addition, the attorneys said that fear of prosecution stifles the speech of online users who are simply role-playing or speaking within their First Amendment rights. **In his brief challenging the California law, Forsyth cites the Supreme Court's 1997 decision** to throw out portions of the federal Communications Decency Act, which made it a felony to display or transmit "indecent" Net content that could be exposed to minors. **The court's majority opinion stated that the statute chilled free speech and that "there is no effective way to determine the identity or the age of a user who is accessing material through e-mail, newsgroups, or chat rooms."** But UCLA's Volokh says that if a Net user states that he or she is a minor, it could be hard for Forsyth to use this age-verification argument to absolve a client. "If indeed he was just having a discussion with someone he thought was 40 and she turned out to be 13, then he would have a strong constitutional defense," Volokh said. **"But if the person said she was 13, and he expressed belief that she was 13, then he doesn't have that defense."**

Security Outsourcing Solutions, Inc.®

One Liberty Square, 6th Floor, Boston, MA 02109 • 100 Ardmore Road, Needham, MA 02494-1833

Guilty Plea - - - As expected, in a bargain with New Jersey prosecutors, David Smith 31, **The New Jersey programmer accused of creating and disseminating Melissa**, pleaded guilty to one charge of computer theft in Monmouth County Superior Court. **He is expected to plead guilty to related charges in federal court in Newark. Smith acknowledged that the Melissa program caused more than \$80 million in damage.** The \$80 million total is related to the time spent by systems administrators to clear the virus off affected computers. **Based on the agreement with Smith's attorneys, New Jersey prosecutors today recommended a sentence of 10 years in prison for Smith**, the maximum of what the law calls for in such crimes. He also faces a fine of \$150,000. Smith is considered to be one of the first people ever prosecuted for spreading a computer virus.

Cyber Squatting - - - The high-tech industry has been flooding Capitol Hill with money and lobbyists, and the effort is starting to pay off. During the first half of the 106th Congress the high-tech lobby was more established and proactive, as proven by legislation that has gained ground or won approval. **The most contested piece of legislation that won passage favors corporations and places new restrictions on so-called cybersquatting.** The provision was buried in a huge federal spending bill. It protects businesses from those who register company trademarks as Internet addresses in "bad faith" and then later try to sell them for a profit. **The provision would outlaw registering "famous" Net addresses such as celebrities' names.** Violators could face between \$1,000 and \$100,000 in fines per domain name. The cybersquatting bill serves as a good snapshot of whose interests are being served by Congress when it comes to the Net, consumer advocates say. **Another bill that was seen as a double-edged sword for consumers** would recognize various forms of digital signatures as a legal way to sign documents. The House and Senate still have to reconcile their versions of the bill. **The version passed by the Senate is more watered down.** It gives contracts signed in a digital format the same legal standing as those signed on paper but doesn't address electronic records. The digital signature bill and other Net-related measures will be taken up when Congress returns after its winter break. But consumer advocates say the tide will continue to favor corporate interests.

Credit Card Scam - - - The U.S. Army Criminal Investigation Command contacted the U.S. Secret Service, about the misuse of personal identity information that individuals had posted on the World Wide Web. **The perpetrators took information culled from the Congressional Record**, a publication chronicling the legislative deliberations of the U.S. House of Representatives and the Senate, that included the names and social security numbers of officers who were up for promotion. **Senate approval is required for the promotion of major and above, and the names and social security numbers of eligible officers** were submitted to the Armed Services Committee, which sanctions the promotions. The information was then posted on a Web site where others could take advantage of the data to apply for unauthorized credit under victims' names. The Pentagon no longer forwards social security numbers to Congress. **On December 13, Secret Service agents in conjunction with the Trenton Police Department** arrested Lamar Christian and Nevison Stevens in Trenton, NJ and Ida Johnson- Christian, in Pennsylvania. A Secret Service press release identified over 700 unauthorized accounts that were available for **fraudulent e-commerce purchases**. According to Special Agent in Charge Peter A. Cavicchia II, of the Secret Service this particular ring had used 113 of these accounts and precipitated \$37,000 in actual losses. **Potential losses were estimated at \$1.4 million.** The arrested subjects are being charged **with conspiracy to commit bank fraud in violation of Title 18 of the United States Criminal Code, Section 371.** The maximum penalty for violation of this statute is 30 years imprisonment and a fine of not more than \$1 million. District attorneys in Delaware, New Jersey and Pennsylvania will prosecute the case.

Telephone Scam - - - If you receive a telephone call from a person identifying them self as an AT&T service technician and the person informs you that they are running a test on your line, beware. The caller will then instruct you to touch 9, 0 and the pound (#) sign and hang up to complete the test. **By dialing 90 # your giving the person that called you access to your telephone line.** By dialing 90 # and hanging up the person that called you can make a long distance telephone call anywhere and the charge will appear on your telephone bill. **The scam has been originating from jails and prisons.**

Visit our Web Site!

www.security-outsourcing.com

Espionage - - - Software that allows a computer to receive radio signals could make spying on other computers all too simple, according to two scientists at the University of Cambridge, in England. Such are the dangers that they are patenting countermeasures that computer manufacturers can take to foil any electronic eavesdroppers. Its no secret that it is already possible to read documents written on computers by intercepting the radio-frequency emissions from their electronics, **but the tuning and antenna equipment needed to do this is not available off-the-shelf and is expensive.** But a new breed of “**software radio,**” designed to let computers tune in to radio signals in any waveband, promises to make this type of eavesdropping **simple and cheap.** A PC circuit board with a plug-in aerial does all the tuning under software control and has a digital signal processor chip to cut noise. “Equipment to do this [EAVESDROPPING] would now cost in the area of 30,000 pounds, however, in five years it will cost less than 1000, and it’s hackers, who will be writing the software,” **predicts Markus Kuhn,** a research student who has filed the patent with Cambridge cryptographic expert Ross Anderson.

Credit Card Fraud - - - **John Faughnan, a 40-year-old Minnesota physician,** was leafing through his Visa bill in **December 1998** when he spotted an **insignificant** \$19.95 charge from a company called **Webtel.** He’d never heard of Webtel. Curious, he dug up his old bills: **he had been hit for exactly \$19.95 once a month for six months, like clockwork.** So Faughnan began investigating online, following a paperless trail of corporate registrations and a maze of mail drops. Meanwhile, the Federal Trade Commission had been investigating as well. **On January 12, 1999, the FTC filed civil charges against one Ken Taves, two other people, and Taves' eight businesses,** freezing his personal assets and placing some of the companies under temporary receivership. Receivers and regulators are floating mind-boggling figures: **900,000 consumers victimized in 20 countries, \$45 million in profits, \$19.95 at a time.** Taves' companies handled billing for adult Web Sites, but that didn’t explain everything. “Many consumers either do not have access to the Internet or have not given their card information over the Internet,” the complaint charges. “Some consumers do not even have a computer.” **Where did the credit card numbers come from? The FTC doesn’t have the answer,** but Faughnan, the computer underground, and the publishers or this newsletter can guess. Credit card numbers are formed with a well-known algorithm, and programs to generate potentially valid numbers are easily found online. If a well-formed number is successfully billed, then a scam artist could have a computer automatically bill it again, month after month. For now, Taves is cooling his heels in the Federal Metropolitan Detention Center in Los Angeles. The FBI arrested Taves on May 4. He is charged with lying to the FTC about his assets, and disobeying a court order requiring him to hand over about \$6 million from his secret bank account on the Grand Cayman Island. Taves is also held on a probation violation, but the government hasn’t charged him with criminal credit card fraud. The FTC action is purely civil, and if the trial happens, it will be all about money. After dabbling in petty scams for a decade, Taves seems to have hit it big in e-commerce. The charges holding him now are minor, and the FTC may well lose its civil suit against his formidable legal team.

Crime Blotter - - - Three blind Arab brothers in Jerusalem tapped into Israeli army telephone lines and enabled Palestinians in the West Bank and Gaza to call overseas at the military’s expense. Using Braille keyboards, Munther Badir, 22, Muzhir Badir, 23, and their younger brother, a minor who cannot be identified, committed 42 counts of computer fraud, according to prosecutor Doron Porat. **“This is the first crime of this sort to be brought to trial in Israel,”** Porat said of the brothers, who have been blind since birth and deny any wrongdoing. Besides cracking the codes of a military switchboard and charging Palestinians a fee for the calls abroad, the brothers jammed the telephone lines of a brothel— apparently as a favor to a competing establishment across the street, prosecutors said. **Porat said the brothers were making more than \$10,000 a day at the peak of their alleged exploits.** The trio also hacked into the computer of Israel’s cable shopping channel and had a 25-inch television sent to their home for free, according to the charge sheet. Muzhir Badir said in a telephone interview from his home, where he is under house arrest, that he and his brothers had only wanted to demonstrate that the blind were as talented as people with sight. “In the Arab community, blind people are considered the last people who could contribute to society,” Muzhir said. “We wanted to prove from the very beginning that we were special.”

LOGIN TO...SOS-DueDiligence.com

Now you can obtain Due-Diligence Investigative Price Quotes — Online — 24 hours a day/7 days a week! SOS-DueDiligence.com is committed to providing professional investigative services in a cost effective, efficient and timely manner. SOS-DueDiligence.com allows you to make informed business decisions regarding mergers, acquisitions, investments, litigations, or to simply establish a business relationship. Compare our prices with those you are currently paying for investigative Due-Diligence services.

- **RISK ASSESSMENT INQUIRY (US Only)** provides a snapshot evaluation of a company's credit worthiness and legal corporate status. *Recommended as a business to business fraud detection and prevention tool.*
- **BUSINESS ASSESSMENT INQUIRY (Global)** provides information about a company, its officers and directors, legal issues, etc. *Recommended for corporate and financial transactions, civil litigation, suspected fraud or other criminal activities, and evaluating prospective clients and partners.*
- **COMPREHENSIVE BUSINESS ASSESSMENT (Global)** provides in-depth information about a company, its officers, directors, subsidiaries, corporate affiliations, finances, reputation, etc. *Recommended for mergers, acquisitions, civil litigation, investments and competitor assessments.*

Visit our Web Site today to learn more about our investigative Due-Diligence services.

SOS-DueDiligence.com, the leader in providing business to business informational tools for the 21st century.

Corporate Homicide is a newsletter published for the exchange of information, ideas, theories, and related topics, and may not be construed as legal advice. The information provided is "general information," not "specific advice." We refer you to your professional legal and/or security providers for required services or specific advice. The publisher does not necessarily endorse opinions expressed by contributors. The publisher and any re-publisher cannot be held responsible for any loss incurred as a result of the application of any information published in the Corporate Homicide Newsletter.

*Circulated quarterly to businesses. To receive future issues please register at www.security-outsourcing.com by completing the **Ask the Experts form**. Also specify if you would prefer to receive Corporate Homicide via e-mail. Feedback and suggestions on future topics are welcome. © 2000. Security Outsourcing Solutions, Inc.®*



SECURITY
OUTSOURCING
SOLUTIONS, INC.®

One Liberty Square, 6th Floor • Boston, MA 02109

January 2000

CORPORATE **HOMICIDE** LIFE IN A GLOBAL ECONOMY™

A NEWSLETTER FOR THE SECURITY AND NON-SECURITY EXECUTIVE