



CORPORATE HOMICIDE™

LIFE IN A GLOBAL ECONOMY

A NEWSLETTER FOR THE SECURITY AND NON-SECURITY EXECUTIVE

Drug Testing - - - It's natural. It's organic. It's composed of 100 per cent recycled materials and, most important to his customers, it's guaranteed drug-free. For \$69 (U.S.), plus postage, Kenneth Curtis sells five ounces of his urine in a little plastic bag, along with 30 inches of plastic tubing and a tiny heat pack designed to keep his fluid at body temperature. Taped to the body, this "urine test substitution kit" enables customers to pass off his urine for their own during workplace drug tests, which are commonplace in the U.S. Last spring, irate that Curtis' kit could foil drug tests, South Carolina State Senator David Thomas drafted a bill to ban the sale of urine. The bill carried a penalty of five years in prison for selling urine — or even giving it away — with the intention of defrauding a drug test. Texas, Nebraska and Pennsylvania had already enacted similar bans. Curtis' kit works, which really irks South Carolina's Senator Thomas. "Urine testing is easily fooled by what this man is doing," he said. "Their technology is beating our technology right now."

Evidence Tampering - - - In an effort to protect company secrets and client information from prying eyes Disappearing Inc., a start-up software company says it has created a "**self-destruct**" mechanism that allows e-mails to disappear without a trace. The new technology works with any e-mail system to encrypt, authenticate, track and delete messages, including those stored on backup tapes or forwarded to third parties. The software encrypts each message with a unique key to prevent unauthorized access. Receivers then authenticate themselves in one of several ways before viewing a message. There is a record of all access, and when a particular key is destroyed, the message becomes unreadable. By eliminating the permanent record of virtual conversations, says the company, they are making e-mail safe and more secure for business. The software will debut early next year. An unintended side effect of the new software, which is designed to guard and promote e-commerce, may be to further mask the identities of cyberstalkers and online pedophiles. With Internet crime on the rise and e-mail messages used as evidence and as a way to track suspects, the new technology poses potential problems for police and prosecutors. Disappearing Inc.'s e-mail management system works no matter what e-mail program the sender and receiver of a message is using, including Web Mail, Microsoft Outlook, and Netscape Mail. According to the company, users will not notice any changes to e-mail programs.

Identity Fraud - - - Travelers Property Casualty Corp., the number three U.S. property and casualty insurer, has launched insurance coverage for victims of identity fraud — the first of its kind. The identity-fraud coverage offers policy holders up to \$15,000 of expenses they incur in clearing their name and correcting their financial records after a fraud, Travelers Property said in a statement. The company's 2 million homeowners or tenants insurance policy holders can get the new fraud coverage for just \$25 a year on top of their average annual premium of \$450. The new type of policy includes reimbursement for legal expenses, loan reapplication fees, telephone and certified mailing charges, notary expenses and lost wages for time taken from work to deal with the fraud. Travelers Property said the average identity thief runs up \$20,000 to \$30,000 in bills. The victim is generally not liable for bad debts. But Travelers Property said the new insurance coverage was aimed at compensating the victim for money spent in redressing the damage caused.

Prosecution - - - Data obtained from the Department of Justice under the Freedom of Information Act found that of 419 cases of alleged computer fraud referred to federal prosecutors last year, only 83 cases were prosecuted. Federal prosecutors, usually for lack of evidence, dismissed the remainder.

That prosecution rate has held steady since 1992, even as the number of cases has tripled. Every year between 64 percent and 78 percent of federal computer fraud cases are tossed out or sent to the states for prosecution. That means police are obtaining search warrants, investigating alleged crimes and making arrests in cases that are too weak to prosecute on the federal level.

Wiretap - - - If you're finding user-installed cameras and/or microphones on Windows NT machines in your enterprise, be afraid. U.S. Army special agents have been showing their commanding officers how to turn microphones and cameras into remote spying devices. "**We run this in the lab here all the time.** You can hear the guys talking [from another room], but they have no idea you're listening to them," said Jeff Hormann, special agent in charge of the Computer Crime Resident Agency, U.S. Army Criminal Investigation Command, Fort Belvoir, VA. **The attack is delivered to the victim as a Trojan horse — a hostile applet carrying executable code — via an e-mail attachment.** Once the attachment is opened, the attacker, using ports 12345 and 12346 on the desktop, or via HTTP Web protocol and file transfer protocol connections, can load a remote administration tool and order the Trojan horse to turn on the video and/or audio of the targeted machine. By exploiting remote administration tools such as NetBus and Back Orifice, both of which the Army has proved can be used, the attacker can hijack desktop camera and microphone applications and then direct image and voice transmissions to the attacker's PC. **Worse, said Powell Hamilton, manager of technology risk services at PricewaterhouseCoopers in Los Angeles,** attackers can use the same tactics to hijack an online meeting session conducted through systems like Microsoft Corp.'s NetMeeting and grab shared whiteboard information.

There's a warning that bears repeating: Keep virus- and intrusion-detection tools up-to-date. Symantec Corp.'s Norton AntiVirus, for example, recognizes when NetBus 1.6 and 2.0 and Back Orifice and Back Orifice 2000 are running on a desktop. Given the voyeuristic ways of hackers and rising concern over electronically committed corporate espionage, now is a good time to take inventory of your organization's microphones and cameras. **If users have deployed these devices, teach them to manually cap cameras and unplug microphones when not in use.** And if your organization is moving toward adoption of voice and video technologies, pay for higher-end microphones and cameras with indicator lights.

Hijacking - - - The Federal Trade Commission announced a crackdown on Internet operators who hijack Web pages by redirecting users from an intended Web page to a site displaying pornography and adult ads. **The enforcement effort is aimed at stopping an electronic version of the old "bait and switch" game,** in which operators copy existing Web sites and insert coded instructions using JavaScript into the bogus sites, automatically redirecting users to adult sites.

In the process, a user's "back" and "forward" commands on the Web browser are disabled, creating an endless cycle of being trapped. The only way out is to close the browser. Federal authorities refer to this scam as "pagejacking" and "mouse trapping." **These operators hijacked Web sites, kidnapped consumers and held them captive,** said Jodie Bernstein, director of the FTC's Bureau of Consumer Protection. "They exposed surfers, including children, to the seamiest sort of material and incapacitated their computers so they couldn't escape." **Bernstein estimated that as many as 25 million Web pages** from sites as diverse as the Harvard Law Review and the Japanese Friendship Garden have been copied. Hijacking Web sites works like this: operators make exact copies of the Web pages and then change part of the Web page's embedded text, which is hidden from view but checked by online search engines, when looking for a Web site. Bernstein speculated, that since these sites charge for banner ads, the traffic generated by the "kidnapped" Web surfers means more hits and more money in the hands of the operators. **David Landrigan made the discovery of the hijacked Web sites, a professor at the University of Massachusetts at Lowell,** who found hundreds of pilfered Web sites. He said he was "gratified" to see the FTC taking this action.

Fingerprinting - - - Scientists report that a new electronic method for “fingerprinting” credit cards may be effective enough to ultimately take a bite out of the \$1 billion-a-year card-counterfeiting and fraud racket. The system is based upon an accidental discovery that every piece of magnetic media — including the strips used on the back of credit cards — has its own unique background noise patterns that can be “read” with special equipment. “We’re amplifying the signal 100 times until we’re able to see its unique background noise,” said Robert Morley, an associate professor of engineering at Washington University. **In a nutshell, it allows us to determine whether the magnetic strip is the original or a copy of the original.** The unique electronic noise patterns of a specific piece of magnetic media cannot be duplicated — even when thieves copy the data from the magnetic strip of a legitimate credit card and transfer it to phony credit cards. The hope is that by modifying existing credit card readers, banks and merchants may be able to routinely detect and reject bogus cards, researchers say. The university has licensed the technology to Mag-Tek, a California company. Working with a major card company that it will not identify, Mag-Tek plans to test the technology in 1999 and hopes to have it on the market by 2000.

Workplace Violence - - - Two New DCC, Inc. Guides Provide Critical Information for Employers and Employees on How to Recognize the Warning Signs of Workplace Violence and on How to Protect Themselves. **DCC has introduced two new LifeCare Digests on workplace violence**, designed to help both employers and employees recognize, prevent and deal with these incidents. **A LifeCare Digest For Employers: Preventing Workplace Violence**, is geared toward HR professionals and managers and provides basic information on risk factors, warning signs, and strategies including providing employee conflict resolution training, peer counseling and employee assistance programs (EAPs) for employees. **A LifeCare Digest On Preventing Workplace Violence is geared toward employees** and provides helpful tips and information on recognizing warning signs, avoiding potential “danger zones” and taking safety precautions. “Management is beginning to understand that the rampage-type attacks by a disgruntled employee are not the primary threat to their employees,” said Peter G. Burki, CEO of DCC Inc. “Conflicts, threats, harassment and intimidation are recognized as the greatest risk to American workers. Founded in 1984, DCC® is a global provider of critical workplace services that increase productivity and efficiency and reduce absenteeism, turnover and stress. (<http://www.dcclifecare.com>)

Crime Blotter - - - In a Dallas federal courtroom, Calvin Cantrell stands silently, broad shoulders slouched. He was part of a ring of hackers that pleaded guilty to the most extensive illegal breach of the nation’s telecommunications infrastructure in high-tech history. The case demonstrates that hacking’s potential harm is far more ominous than theft of telephone credit-card numbers. Cantrell was part of an 11-member group dubbed ‘The Phonemasters’ by the FBI. They were all technically adept twentysomethings expert at manipulating computers that route telephone calls. **The hackers had gained access to telephone networks of companies including AT&T Corp., British Telecommunications Inc., GTE Corp., MCI WorldCom (then MCI Communications Corp.), Southwestern Bell, and Sprint Corp.** They broke into credit-reporting databases belonging to Equifax Inc. and TRW Inc. They entered Nexis/Lexis databases and systems of Dun & Bradstreet, court records show. **The breadth of their monkey wrenching was staggering;** at various times, they could eavesdrop on phone calls, compromise secure databases and redirect communications at will. They had access to portions of the national power grid and air-traffic-control systems, and had hacked their way into a digital cache of unpublished telephone numbers at the White House. Cantrell and some friends had managed to get their hands on some telephone numbers for FBI field offices. **They entered the telephone system and forwarded some of those FBI telephones to phone-sex chat lines in Germany, Moldavia and Hong Kong.** As a result of the prank, the FBI was billed for about \$200,000 in illegal calls. Unlike less-polished hackers, they often worked in stealth, and avoided bragging about their exploits. **Their ultimate goal was not just fun but profit.** Some of the young men, says the FBI, were in the business of selling the credit reports, criminal records and other data they pilfered from databases. Their customers included private investigators, so-called information brokers and — by way of middlemen — the Sicilian Mafia. According to FBI estimates, the gang accounted for about \$ 1.85 million in business losses. **The Phonemasters often got passwords and other key information on companies in a low-tech approach called ‘Dumpster diving,’** raiding the trash bins of area phone firms for old technical manuals, phone directories and other company papers. This often allowed Cantrell to run one of his favorite ruses — passing himself off as a company insider. Cantrell was sentenced to two years in federal prison.

Cyber Stalking - - - When Jane Hitchcock complained about an advertisement from a literary agency, she didn't expect more than three years of harassment in cyberspace — phone calls from strange men wanting to share their sex fantasies. But that's just what happened to the former Maryland resident after "**cyberstalkers**" began posting troublemaking e-mails and messages about her on the Internet. Testifying before Congress, Hitchcock urged lawmakers to expand current anti-stalking laws to address the new and growing phenomenon of cyber stalking. **One "cyberstalker" invited people around the world** to call or mail Hitchcock their sexual fantasies to help her write a book. The message included Hitchcock's real telephone number and home address. "I began receiving 25 to 30 phone calls a day from as far away as Germany," Hitchcock told the House Judiciary Committee's crime subcommittee. "That's the point where I decided I had to call police and ask for help." But law enforcement offered little help, she said. So Hitchcock turned to friends who knew how to track the origin of e-mail. They traced the messages back to three people who apparently were connected to the literary agency, she said. **She filed a \$10 million civil suit against the three.** Soon after, her lawyer received a death threat. The suit is still pending. Hitchcock urged Congress to pass a bill that would strengthen federal laws designed to fight all types of stalking that involves crossing state lines. "**'Cyberstalking' is something I wouldn't wish on anyone,**" she said. "I felt like someone had broken into my house, touched all of my things, didn't take anything and left. I felt violated and scared for my life." **Rep. Sue Kelly, the New York Republican who sponsored the 1994 anti-stalking law,** said she would seek to broaden the federal definition of stalking to include e-mail and telephone calls.

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. ©1999. Security Outsourcing Solutions, Inc.*



SECURITY
OUTSOURCING
SOLUTIONS, INC.®

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

October 1999

CORPORATE **HOMICIDE** LIFE IN A GLOBAL ECONOMY

A NEWSLETTER FOR THE SECURITY AND NON-SECURITY EXECUTIVE