The Information Security Year in Review: 1995

M. E. Kabay, PhD, CISSP

Security Leader, INFOSEC Group, AtomicTangerine, Inc.

Security awareness is growing; 1995 has been a year of increasing attention to protecting information assets. Herewith, some of the year's highlights in InfoSec:

1 January:

A British teenager hacked into sensitive U.S. government computers and was able to monitor secret communications over the North Korean nuclear crisis in the spring of 1994. The lad tapped into several defence computers for seven months in what U.S. officials conceded was one of the most serious breaches of computer security in recent years.

In another development, Chinese authorities expressed dismay over the growing availability of pornographic computer games, especially in the industrialized coastal areas of this vast, repressed territory. A major credit-card fraud ring was dismantled in Hong Kong and Shenzen, with hundreds of bogus cards and card-making equipment plus account data found and destroyed. Each bogus card was for sale in Hong Kong for about U$250. China also announced major efforts to shut down its flourishing criminal exploitation of intellectual property--illegal copies of software, music and video products.

Newark Airport, the 10th busiest in the U.S. lost power from 17:00 overnight and disrupted air traffic throughout the continent when construction crews damaged three major cables.

A New York state senator introduced legislation that would jail paedophiles who make contact with children on computer networks after a 51-year-old man posing as a teenager exchanged sexually explicit material in cyberspace with a 14-year-old girl and was stopped by the child's mother as he walked with his victim through a shopping mall.

Mark Abene, known to the underground as "Phiber Optik" was released from jail and treated to a hero's welcome by admirers of criminal hackers.

The National Computer Security Association hosted the Second International Conference on Information Warfare(IW2) in Montreal. Attendance was over 80, compared with the from the 63 who attended IW1. In September, the NCSA's IW3 (in Washington, DC) had over 400 participants.

The Computer Emergency Response Team Coordination Center (CERT-CC) at Carnegie Mellon University in Pittsburgh, PA reported major attacks on Internet firewalls using the well-known technique of "IP packet spoofing."

In Philadlphia, plumber Michael Lasch ordered remote call-forwarding for several phones--none of which he owned. He managed to divert calls to at least five rival plumbing

companies to his own service. To add insult to injury, he rudely dismissed unprofitable calls to his rivals, causing one irate customer to call the original plumber back with a complaint--and thus to the discovery of the scam.

2 February:

In Washington, law enforcement officials described food stamps as "the currency of fraud" and pushed for better electronic benefits systems and stronger requirements for identification. Total losses to fraud in the U$26 billion program may amount to about $1 billion per year.

Vandals from the "No Connection" anarchist group disrupted flights at Frankfurt airport in Germany by slicing through three fiber optic cables needed for computer networks. The airport itself, several airlines, and adjacent medical clinics were affected.

A Japanese bank employee and two computer operators were arrested and charged with using PCs to steal about U$1.4 million from Tokai Bank Ltd by making fraudulent bank transfers. Their attempt to transfer U$14.9 million was discovered and aborted by bank officials.

A growing wave of "slamming" erupts in the U.S. as small telephone companies illegally switch consumers' phone services to their own companies--with up to 300% increases in rates. In Los Angeles, prosecutors launch a U$6 million lawsuit against Sonic Communications Inc to punish them for the practice.

In Portland, OR, four thieves withdrew U$346,770 on a single stolen bank card while system software was being updated. Unfortunately, the changes meant that normal U$200/day limits were no longer imposed on withdrawals.

Jake Baker, a University of Michican student was charged with posting messages on the Internet describing the binding, rape, torture and murder of a woman who used to be in his class. He defended his action by claiming that they were not illegal. The case against him was eventually expanded because of even worse postings advocating violence against women but dismissed in June on the basis of First Amendment rights. Federal prosecutors appealed that judgement in November.

Criminal hackers planted Trojan software on the CapAccess Internet provider in Washington DC. The software logged user IDs and passwords and resulted in two days of downtime as sysops repaired system security for its 12,000 compromised users.

In Washington, DC, a federal judge ruled that the National Security Council must

preserve its electronic mail records and make them available to the public within the same guidelines as paper documents.

Notorious phone phreak and criminal hacker Kevin Mitnick was arrested in Raleigh, NC after two years as a fugitive from justice. He was ordered held without access to the phone system. In July, he reached a plea bargain with prosecutors and accepted eight months in jail.

A French judge received evidence that anti-terrorist police at President Francois Mitterrand's palace illegally bugged the phones of journalists and politicians.

A 13-year-old daughter of a hospital clerk was arrested for calling seven discharged patients to tell them they had tested positive for the AIDS virus. One adolescent tried to kill herself as a result. The perpetrator gained unauthorized access to medical systems through an unsecured terminal in her mother's office.

3 March:

San Diego police warned the public that thieves are using electronic monitors to intercept and decode signals from automatic garage-door openers and car alarm systems. The thieves then play back the coded signals and open the doors without trouble.

In Israel, someone posted the identity of Israel's chief of secret police (top secret information) and posted it on the Internet. Great embarrassment in the government....

France reated a new body to protect its economic secrets and advise French firms and the government on trade strategy in a world increasingly engaged in information warfare.

Two criminal hackers were sentenced to federal prison for defrauding MCI and other telephone carriers of more than U$28 million. One of the pair became a mole by getting hired as a technician at the MCI offices in Carey, NC. He implanted illegal software which recorded 50,000 credit card and phone card numbers and fed the data to European confederates who stole telephone services using these accounts.

4 April:

Netscape Communications Corp., America Online Inc., CompuServe Inc., Prodigy Services Corp. and International Business Machines Corp. announced that they are backing Terisa Systems in developing the Secure HyperText Transfer Protocol based on the combined work of Enterprise Integration Technologies Corp. and RSA Data Security Inc.

U.S. Marshals in Lexington, Kentucky raided one of the world's largest pirate bulletin boards (BBS), Assassin's Guild for software piracy. Home of Pirates With an Attitude (PWA) and Razor 1911, the state-of-the-art BBS offered hundreds of pirated software programs. U.S. Marshals seized 13 computers, 11 modems, a satellite dish used for high-speed data transfers, 9 gigabytes of on-line data and 40 gigabytes of backups.

In a survey of 3000 students enrolled at University of Dayton and Wright State University in Ohio, 95% of the business students admitted having cheated in high school and college courses. Other surveys reported in scholarly journals indicates that 60% of high school students cheated on exams within the past year; more than 33% of college students polled also admitted cheating.

5 May:

The German government ordered mobile phone operators to arrange for easy eavedropping on cellular phone calls by police. Each of the three firms affected would have to invest about 50 DM million (U$36 million) to upgrade their digital mobile phone network.

In Salt Lake City, UT, a 15-year old boy was arrested after selling over $10,000 of nonexistent computer parts to gullible victims who responded to his Internet advertisements. The boy's parents were apparently unaware of his activities.

The FCC announced a crackdown on fraudulent advertising that suckers victims into making long-distance calls to off-shore answering machines--and then having foreign telephone companies sock them with big bills. The growing scams, mostly centered on locations in the Dominican Republic, Guyana and Sao Tome; the foreign telcos pay a kickback to the fraudulent operators of these services. Losses average a few million U$ a month so far and are getting worse.

MasterCard International Inc. announced an agreement with the Los Alamos National Laboratory of the Department of Energy of the U.S. to develop more sophisticated artificial-intelligence programs for spotting credit-card fraud. The neural-net programs are supposed to help identify unusual or suspect uses of credit cards and would eventually signal human monitors to ask for better identification before authorizations are granted.

In Melbourne, Australia, federal police arrested two phone phreaks and charged them with stealing phone services. Forty-four other people were interrogated in the operation aimed at breaking an extensive phone-fraud ring.

According to The Sydney Morning Herald newspaper, Japanese agents spied on at least nine Australian missions, including using an infra-red beam to eavesdrop on their embassy in Jakarta. Australian counter-intelligence officers were said to have issued warnings to its diplomats in east Asia to watch out for further espionage.

San Jose, CA prosecutors announced indictments in a case of industrial espionage in Silicon Valley. Two executives of the defunct Semiconductor Spares Inc. were charged with stealing over 500 technical drawings from Lam Research Corp. More indictments were planned.

Also in San Jose, the FBI announced that it had cracked a ring of computer-chip thieves, arresting 15 people in Prestige Computer Inc. alleged to be planning a multimillion dollar raid on an Intel Corp. warehouse containing the sellable, untraceable chips. Chip manufacturers announced later in the year that they would cooperate to imprint chips with traceable serial numbers to cut down on the growing traffic in stolen processor and memory chips.

The New York Supreme Court shocked the on-line world when a judge ruled that Prodigy, one of the big three on-line service providers, was responsible for libellous messages posted on one of its forums. The ruling was particularly disturbing because Prodigy had made good-faith efforts to screen offensive materials; the judge wrote that these very efforts made the service more liable for damages than competitors such as CompuServe and America Online Line where less stringent review of posted material is common. The case went on into the appeals process.

A big fuss erupted over false claims that Microsoft's Registration Wizard for Windows95 would automatically forward system configuration data to the software giant's databases. In fact, the registration software simply offers users the possibility of sending such data during the registration process.

An angry employee at Initial Healthcare Services in London, UK hacked into his employer's computers and generated official letters on company letterhead and signed with forged signatures to announce that each of the 100 employees had been fired. Some of the victims of this bizarre prank even received fraudulent cheques ostensibly as part of their termination of employment.

6 June:

In Gloucester, UK, a supermarket clerk was convicted of having caused months of confusion and extensive wasted effort by sabotaging his employer's inventory database to make it appeat that there were 22,000 Pounds of missing inventory. He damaged the data on his last day of work.

In London, UK, police questioned 14 teenagers who apparently used a detailed crime manual located on the Internet to perpetrate credit-card fraud. "The Internet is a horrible monster that's been created and we can't do anything about it," said London Detective Inspector Ron Laverick. "It's out of control." Six teens were arrested for having used credit card numbers gleaned from the Internet to order thousands of Pounds of electronic equipment.

The American Cancer Society accused the tobacco industry of espionage when internal documents from the Philip Morris Co. revealed that the tobacco giants had obtained working papers from the medical group in the 1980s to counter efforts to publicize the dangers of tobacco.

In a landmark event for cybernauts, the U.S. Senate voted 84 to 16 to ban "obscene" material from computer on-line services, including the Internet. The Communications Decency

Act, known as the "Exon-Coats Bill," would establish penalties of fines of up to U$100,000 and two years imprisonment for people who "knowingly make, or make available" obscene communications, or send indecent material to minors across electronic networks. The Net erupted with protests and frenzied discussions of the implications of this bill. Noted liberal Newt Gingrich came down against the bill.

In Spain, CESID, the military intelligence service, was accused in front-page newspaper reports of illegally listening to the telephone conversations of the king, a top soccer figure and other luminaries. The announcement created a furore in the country.

Great American Insurance Co. of Cincinnati, OH agreed to pay U$266,436 to purchase legitimate copies of proprietary software found on its computers in an audit by the Business Software Alliance. Although the company had policies in place against software theft, they were not enforced. The cost of embarrassment to the company was not calculated.

Europay International SA, the largest credit-card system in Europe, announced in Berlin a joint venture with IBM to help make electronic payments more secure on the World Wide Web by supporting smart cards.

Cellular phones are banned at several hospitals after innocent phone users cause havoc with remote sensing units. Medical and nursing staff report multiple cases of panic calls such as cardiac arrests when the phones output scrambles sensitive medical electronics.

In the Washington, DC area, Scan International Corp. furniture stores announced that they would no longer accept cash--only credit cards and cashiers' cheques. The plan was a response to a rash of armed robberies in its stores.

Carnegie Mellon University's graduate student Martin Rimm led a team of more than two dozen researchers in the most comprehensive study to date of online pornography. He claimed that pornography is one of the most extensive recreational uses of computer networks and that 83.5 percent of the digitized photos transmitted over Usenet news groups were pornographic. Unfortunately, the study actually dealt with pornographic bulletin board systems, not Internet sites. Further analysis showed serious methodological flaws and outright misrepresentation in Rimm's study. His credibility was lowered even more when it was established that he was writing a book on how to make money by peddling pornography on the Net.

7 July:

Bell Atlantic mailed out 388,000 postcards telling customers their area code changed to 540. Unfortunately, a programming error caused the notices to be mailed to homes in northern Virginia that are keeping the old 703 code. Estimated costs of the blunder: U$100,000.

In Portland, OR Randal Schwartz was convicted of hacking his way into Intel Corp. computer networks in what he claimed was an effort to point out security flaws while he was working there as a consultant. The would-be security expert failed to notify his employers of his intentions and forgot to get authorization for stealing passwords and making unauthorized changes in system software.

The InterNIC, the agency which hands out Internet addresses, finally admitted that the time had come to impose order on the granting of such addresses. Henceforth, organizations claiming the right to use trademarked names would have to provide evidence of their ownership and agree to defend the InterNIC in legal disputes over alleged misuse of such addresses.

8 August:

Federal agents seized $259,700 in counterfeit money from the Lubbok, TX home of a Texas Tech student who apparently used his home computer to print the bills on a colour printer. The fake cash turned up all over Texas and New Mexico.

The U.S. House of Representatives voted 420 to 4 to approve an amendment that expressly prohibits Internet censorship by the government, directly opposing the Exon-Coats bill passed by the U.S. Senate.

President Clinton announced that industrial espionage in the United States by foreign countries may cost Americans billions of dollars a year and pose "a serious national security concern."

The Church of Scientology succeeded in having U.S. Marshals seize computer equipment from a many they accuse of spreading its sacred (and copyrighted) texts on the Net. In September, their accusations were rejected by a federal court in Denver.

New York police authorities instituted spot checks on drivers, demanding to see proof that their cellular phones are legitimate. Users were asked to identify their carrier and the monthly subscription fee. Dozens of "clone" phones programmed with stolen codes were confiscated in the first days of the program.

In Las Vegas, DefCon III, one of several criminal-hacker conventions held annually, opened with the hackers' reprogramming of hotel TVs to scroll "Hackers Rule" across the screens. At midnight, participants enjoyed "Hacker Jeopardy"; one answer was "The lowest form of life" and its question was "What are America Online users?"

The world's first widely-distributed macro-language virus made its appearance in MS-WORD for Windows documents. The macro.concept virus demonstrates how to use the macro programming language common to many Microsoft products to generate self-reproducing macros that spread from document to document. Within a few months, clearly destructive versions of this demonstration virus appeared.

The "Hackers" World Wide Web page was hacked by criminal hackers who added hot links to criminal hacking sites where people could pick up pointers on how to steal credit cards and make home-made bombs. In a move that scandalized many security experts, the MGM managers allowed the hacked versions of their material to remain on their site.

9 September:

America Online reported that it was improving security to deal with attacks on its networks and customer files by criminal hackers. The company urged users to change their passwords and never to respond to hackers' on-line requests to divulge those passwords. Security officials admitted that they were having trouble with a widely-available password-cracking program called AOHell.

An on-line sting operation in Newark, NJ netted six arrests and seizure of 20 computer systems when the Secret Service set up an electronic "swag shop" and invited phone phreaks to sell their stolen phone access codes and cellular phone IDs.

In London, UK two men were convicted of fraud by installing a fake automated teller machine on the wall of a legitimate business. The machine always accepted the victims' bank cards and recorded their account codes and the PINs entered in response to prompts. The thieves stole 120,000 Pounds using the purloined codes.

A Chicago court heard demands by a resort owner and a scuba instructor alleging defamation by an anonymous user of America Online. The plaintiffs demanded that AOL reveal the name of the user so they could sue the individual for libel. This case is the first to deal openly with a serious issue in cyberspace: the link between anonymity and irresponsibility.

Two young criminal hackers accused of tapping into Tower Video stores nationwide and collecting information on 2,000 credit card accounts were indicted by a federal grand jury in Sacramento, CA. The accused apparently stole the information and then tried to cover their penetration by deleting log-file records.

In a meeting in Washington, DC government and industry representatives found no common ground on the question of strict controls over export of strong encryption. The International Traffic in Arms Regulations continues to govern such exports, to the annoyance of many business users of encryption.

The French media jumped on a story in the satirical Le Canard Enchainé newspaper which reported that criminal hackers successfuly tapped into a navy computer system and gained access to secret French and allied data, including secret "acoustic signatures" for warships.

Netscape security algorithms were cracked by two graduate students who posted their findings on the Net. Netscape Communications Corp., which provides secure communications for financial transactions on the Internet, responded immediately with fixes.

A lunatic in the Manchester and Newcastle air-traffic control areas broadcast false instructions to pilots, resulting in extreme danger to everyone in the air and under the flight paths.

News broke of a criminal hacker attack on Citibank's computerized cash-management systems. Russian hackers apparently succeeded in siphoning about U$10 million into foreign banks, but bungled their attempts to extract cash from these electronic, fraudulent deposits. All but U$400,000 of the stolen funds were recovered.

The National Computer Security Association's Third International Conference on Information Warfare welcomed 450 participants to Washington DC to discuss the growing field of analysis. Participants discussed such issues as the future of criminal hackers in the workplace and the need for national and international action to prevent damage from information warriors.

10 October:

Security flaws in HotJava 1.0 alpha 3 release alarmed many in the information security community and the Net at large. HotJava from Sun Microsystems is a new program for enhanced World Wide Web communications, and the specific version allowed man-in-the-middle attacks, where observers could capture all traffic between a user and a Web site.

11 November:

Christopher Pile became the first person convicted under Britain's Computer Misuse Act of 1990. Pile created several widespread computer viruses, including Pathogen and Queeg. He was sentanced to 18 months in jail.

12 December:

America Online hit the news again when its automated screening software banned the word "breast" in its attempt to clean up pornography on its network. Unfortunately, victims of ****** cancer found themselves unable to post discussions of their own disease. Much embarrassment and backtracking by the writers of the screening software.

In California, police arrested 20 people in the largest credit-card fraud ring in the world, accounting for 40% of the U$100 million in annual U.S. losses.

Whitewater witness Jean Lewis complained to the Senate Ethics Committee that her privacy rights were violated when part of a letter she wrote to a friend was read at a Senate hearing last week. The letter was found in the erased portions of a diskette at her place of employment.

The FBI launched an investigation of death threats against actress Jodie Foster which were posted on a Web site in Hollywood.

Cybernauts organized massive protests against the continuing efforts of U.S. congresscritters to impose government controls on content of Internet sites. In the words of UPI writer Linda Dailey Paulson, "The legislation's decency code would make a home page on the World Wide Web meet standards similar to those imposed on Saturday morning cartoons -- standards much stricter than the First Amendment freedoms afforded to print media."