InfoSec Year In Review -- 1999

M. E. Kabay, PhD, CISSP. Security Leader, INFOSEC Group, AtomicTangerine Inc.

Category 11 Breaches of confidentiality

Date 1999-01-29 **Keyword** data leakage privacy confidentiality control Web

Source, Vol, No. RISKS 20 18

The Canadian consumer-tracking service Air Miles inadvertently left 50,000 records of applicants for its loyalty program publicly accessible on their Web site for an undetermined length of time. The Web site was offline as of 21 January until the problem was fixed.

Date 1999-02-03 **Keyword** data leakage Web script QA vulnerability confidentiality

Source, Vol, No. WIRED via PointCast

An error in the configuration or programming of the F. A. O. Schwarz Web site resulted paradoxically in weakening the security of transactions deliberately completed by FAX instead of through SSL. Customers who declined to send their credit-card numbers via SSL ended up having their personal details — address and so forth — stored in a Web page that could be accessed by anyone entering a URL with an appropriate (even if randomly chosen) numerical component.

Date 1999-02-10 **Keyword** e-commerce credit card personal information password privacy

Source, Vol, No. RISKS 20 20

Prof. Ross Anderson of Cambridge University analyzed requirements on the AMAZON.COM online bookstore for credit card number, password, and personal details such as phone number. He identified several risks: (1) merchant retention of credit card numbers poses a far higher risk of capture than of capture in transit; (2) adding a password increases the likelihood of compromise because so many naïve users choose bad passwords and then write them down; (3) even the British site for Amazon contravenes European rules on protecting consumer privacy; (3) such practices make it easier for banks to reject their clients' claims of fraudulent use of their credit-card numbers.

Date 1999-04-08 **Keyword** criminal hacker investigation data diddling

Source, Vol, No. UPI

In East Lansing, MI a criminal hacker broke into a police computer through a faulty Web site and stole information with tips about rioters who trashed the town after "their" team lost a basketball game.

Date 1999-04-22 **Keyword** privacy credit card Web quality assurance ISP Internet Service Provider QA bug error

Source, Vol, No. AP, <http://www.infobeat.com/stories/cgi/story.cgi?id=2559272284-9a6>

Joe Harris, a computer technician at the Seattle-area "Blarg! Online" ISP, discovered that improperly-installed shopping-cart software used widely on the Net to simplify shopping can allow anyone to see confidential data such as credit-card numbers. Security analysts pointed out that the plain ASCII file where such data are stored should not be on the Web server at all, or if it is, the file should be encrypted. Initial evaluation suggested that the weakness affects at least several hundred and possibly many thousands of e-commerce sites where the software installations were improperly done.

Date 1999-04-30 **Keyword** Internet service provider ISP privacy surveillance scans PCs

Source, Vol, No. Reuters

An uproar broke out when Singapore Telecom scanned 200,000 computers belonging to its Internet service customers — without their knowledge or permission. At first, the company hung tough: "We are merely protecting the interest of our customers," said Paul Chong, CEO of Singapore Telecom. Staff explained that the non-invasive scans, carried out by anti-hacker personnel from the Ministry of Home Affairs, did not penetrate systems but merely noted vulnerabilities visible to any hacker. However, the company announced that 900 virus-infected computers had been found — which hardly seems non-invasive. The company apologized to its customers within a couple of days after the furore erupted.

Date 1999-08-26 **Keyword** privacy Web aggregate data collection marketing purchases preferences books

Source, Vol, No. USA Today

The "Purchase Circle" feature of <amazon.com> caused ripples of concern among some observers because it allows anyone to view aggregated purchase data broken down by city, university and organization. Critics argue that knowing which books people in a given competitor are buying may provide valuable competitive information. Amazon responded by providing a way of opting out of participation in the data collection. Legal experts noted that such corporate data collection, publication and use of aggregated data is not illegal.

Date 1999-10-05 **Keyword** criminal hackers crackers theft fraud Web pages sites

Source, Vol, No. BBC MONITORING EUROPEAN - POLITICAL

In late September 1999, Czech police arrested a criminal hacker who was trying to sell stolen personal information about 2.5M users of Internet accounts. The 21-year-old was an employee of the Ceska Sporitelna savings bank and he confessed to the crime.

According to Czech criminal hackers interviewed on Czech radio in October, the state of security on most Czech Web sites is poor; however, the hackers tend to avoid police computers because of possible massive retaliation.

Date 1999-10-16 **Keyword** privacy espionage information warfare confidentiality unlisted ex directory phone numbers gover

Source, Vol, No. Wired

Someone posted several confidential phone numbers for New Zealand government ministers on a home page in the GeoCities Web hosting system. The security breach rendered many home, mobile, and pager numbers unusable as a result of the disclosure.

Category 12 Wiretapping, interception (not jamming; not govt/law enforcement)

Date 1999-04-21 **Keyword** surveillance microphone camera Internet

Source, Vol, No. The Times (London)

According to an article in _The Times_ of London on 1999-04-21, Philip Loranger of the US Army Information Assurance Office demonstrated that unprotected networks with workstations that have microphones or cameras are vulnerable to surveillance.

Category 13 Data diddling, data corruption, embezzlement

Date 1999-01-03 **Keyword** theft fraud hackers bank impersonation crime punishment

Source, Vol, No. RISKS 20 14

Two more Chinese criminal hackers were sentenced to death in China in December 1998. The twin bothers stole 720,000 Yuan (~U$87K) from a bank in Zhenjiang and transferred the money to their own accounts.

Date 1999-04-06 **Keyword** theft surveillance eavesdropping data diddling hacking bank

Source, Vol, No. TIMES OF INDIA

The Times of India reported on the abysmal state of security in Indian businesses, where, as in the rest of the world, managers pay little attention to security until after there's a problem. The article claimed that "a large public sector bank in India was electronically molested recently by hackers who allegedly transferred cash . . . by invading the banks' network."

Category 14 Viruses, hoaxes, Trojans (assembly level or macro: not ActiveX or Java)

Date 1999-01-21 **Keyword** virus contamination sabotage disgruntled employee

Source, Vol, No. Los Angeles Times

Zhang Wenming, a disgruntled Beijing programmer, confessed in January 1999 to infecting 20,000 of copies of educational software with a dangerous virus whose payload included erasing a victim's hard disk. Apparently the 28-year-old self taught programmer was furious at being fired for "poor work habits" and wreaked his revenge on his employer in the last days of his employment.

Date 1999-01-29 **Keyword** Trojan horse backdoor quality assurance QA

Source, Vol, No. RISKS 20 18

Peter Neumann summarized a serious case of software contamination in RISKS 20.18: At least 52 computer systems downloaded a TCP wrapper program directly from a distribution site after the program had been contaminated with a Trojan horse early in the morning of 21 Jan 1999. The Trojan horse provided trapdoor access to each of the contaminated systems, and also sent e-mail identifying each system that had just been contaminated. The 52 primary sites were notified by the CERT at CMU after the problem had been detected and fixed. Secondary downloads may also have occurred."

Date 1999-02-08 **Keyword** virus confidentiality privacy encryption key

Source, Vol, No. RISKS 20 19

The Codebreakers, virus writers with more technical skill than good sense or ethical sensibilities, wrote the Caligula virus, which sends users' PGP secret key ring to their FTP site. This large virus illustrates the dangers of data transfer from inside the firewall and also the stupidity of a legal system that cannot recognize that virus code is not speech and should not be constitutionally protected. Cryptographers recommended that secret-key rings either be stored off the hard disk entirely when not in use or that all data on the disk be encrypted.

Date 1999-02-12 **Keyword** QA quality assurance auditing Y2K consultants fraud embezzle

Source, Vol, No. RISKS 20 21

Bruce Martin pointed out in RISKS that the frantic efforts to remediate the Y2K bugs in production software offer a perfect cover for criminals to insert Trojan code in financial software. Such Trojans could, for example, cause monetary transfers around the Y2K transition out of clients' accounts to the criminals' accounts in offshore banks. The expected confusion at the end of 1999 could cause serious difficulties for auditors as they tried to piece together the reasons for various losses experienced at the turn of the century.

Date 1999-02-25 **Keyword** criminal hackers Internet spam virus denial of service

Source, Vol, No. BBC translation of Bulgarian BTA report

On January 26, criminal hackers attacked the Internet site of the Bulgarian Telecommunications Company in Sofia. The attackers used the site to send virus-infected e-mail [possibly Trojan attachments] to several thousand victims via a US server. On February 5, attackers repeated the spam attack, sending infected e-mail to "a prestigious US college." A few days later, reported the Bulgarian radio service, the BTC e-mail server was subjected to a denial of service spam attack. Luckily, the spam attacks were of sufficiently low volume that users were not inconvenienced.

Date 1999-03-11 **Keyword** information warfare social engineering

Source, Vol, No. RISKS 20 24

An experienced Internet user who happens to use AOL for convenience was shocked to find an e-mail message in his in-basket that contained his AOL password. Moments after opening that e-mail, he as contacted by "Bob SiteOp" using Instant Messaging; this person claimed to be an AOL staff member and demanded to know the contents of the e-mail. The user refused and contacted AOL to no avail -- the staff stonewalled and claimed that AOL does not keep passwords on disk (presumably only one-way encrypted passwords). Despite considerable effort on the user's part, he never received an explanation of what had happened.

Date 1999-03-27 **Keyword** virus e-mail Trojan Outlook address book spam

Source, Vol, No. CERT, news wires

On Friday 26 March, the CERT-CC received initial reports of a fast-spreading new MS-Word macro virus. "Melissa" was written to infect such documents; once loaded, it uses the victim's MAPI-standard e-mail address book to send copies of itself to the first 50 people on the list. The virus attaches an infected document to an e-mail message with subject line "Subject: Important Message From <name>" where <name> is that of the inadvertent sender. The e-mail message reads, "Here is that document you asked for ... don't show anyone else ;-)" and includes a MS-Word file as an infected attachment. The original infected document, "list.doc" was a compilation of URLs for pornographic Web sites. However, as the virus spread it was capable of sending any other infected document created by the victim.

Because of this high replication rate, the virus spread faster than any previous virus in history. On many corporate systems, the rapid rate of internal replication saturated e-mail servers with outbound automated junk e-mail. Initial estimates were in the range of 100,000 downed systems. Anti-virus companies rallied immediately and updates for all the standard products were available within hours of the first notices from CERT-CC.

The Melissa macro virus was quickly followed by the PAPA MS-Excel macro virus with similar properties.

Date 1999-03-30 **Keyword** Excel macro virus e-mail ping denial of service

Source, Vol, No. CERT-CC, news wires

Hot on the heels of the Melissa macro-virus outbreak, a similar virus attacking MS-Excel spreadsheets appeared on the Net at the end of March. The PaPa macro virus was more virulent than the Melissa virus in that it sent out copies of itself to 60 names drawn from the victim's e-mail address book but did so every time an infected document was opened. In addition, the virus launched denial-of-service ping attacks on two IP addresses. The subject line of the automated junk e-mail was "Fwd: Workbook from all.net and Fred Cohen" and the text was "Urgent info inside. Disregard macro warning."

Date 1999-04-01 **Keyword** information warfare virus mail bombing denial of service

Source, Vol, No. Daily Telegraph

The onslaught of the Melissa, Papa and Mad Cow viruses caused significant operational difficulties for NATO military forces in their attacks on the Serbian state. E-mail servers were taken down for disinfection; US Navy ships were infected; and a Belgrade computer tried to swamp NATO e-mail in a simple denial-of-service attack involving 2,000 e-mail messages a day.

Date 1999-04-01 **Keyword** virus writers sociology psychology information warfare

Source, Vol, No. THE DALLAS MORNING NEWS, TEXAS

An article in the Dallas Morning News for April Fool's day quoted Peter Tippett, Sarah Gordon, Winn Schwartau and others discussing the motivations of virus writers and criminal hackers. The experts thought that motivations were complex and varied, that the current crop of virus writers were largely young and less technically sophisticated than the first generation of virus-writing idiots, and that most were probably not malicious -- at least, their intentions were not malicious. Their products often are.

Date 1999-04-02 **Keyword** virus aftermath policies defenses management planning

Source, Vol, No. OTC, AP

The Melissa worm spread explosively through corporate e-mail systems and the Internet in late March. The worm spread through e-mail attachments in MS-Word ".doc" format and mailed itself to the first 50 addresses in each victim's standard e-mail address book. The worm created a false message with a deceptive subject line and content. The worm was traced to virus-writer(s) called "VicodinES."

Date 1999-04-02 **Keyword** virus worm e-mail battle information warfare malicious

Source, Vol, No. Dow Jones, Wall Street Journal

Shortly after the outbreak of the Melissa worm, the Papa worm was released with a component that caused a flood of junk e-mail to the mailbox of Dr Fred Cohen in an attempted denial-of-service attack (foiled by proper configuration management).

Date 1999-04-15 **Keyword** virus defense CERT-CC education reporting

Source, Vol, No. TechWeb

Keith Rhodes, Technical Director for Computers and Telecommunications Accounting and Information Management at the General Accounting Office, warned that Melissa was just a harbinger of trouble to come: "It is likely that the next virus will propagate faster, do more damage, and be more difficult to detect and to counter." He urged software makers to take responsibility for providing better protection in their own products against malicious code. Michael Vatis, Director of the FBI's National Infrastructure and Protection Center, warned, "Because of the ease of writing and disseminating destructive and disruptive viruses, deterring people from engaging in such conduct is the surest method of prevention." Richard Pethia, Director of Carnegie Mellon University's Computer Emergency Response Team Coordination Center at the Software Engineering Institute <http://www.cert.org> argued that only fundamental redesign would accomplish this goal. Currently, software such as MS-Word has extended its functionality at the expense of security. But Pethia added, "If we're ever faced with simultaneous infections at Internet speed, we won't be able to handle it." Only secure default configurations, strong identification and authentication and integrated virus resistance will prevent future disasters due to portable executable code.

Date 1999-04-26 **Keyword** Chernobyl virus CIH perpetrator virus writer history

Source, Vol, No. News wires

According to news wire reports, the Chernobyl computer virus struck hundreds of thousands of computers in Asia and the Middle East, with Turkey and South Korea each reporting 300,000 computers damaged on 26 April. Singapore reported more than 100 cases of infection by the Chernobyl virus (AKA CIH or Space Filler) on that date, the anniversary of the nuclear plant meltdown in 1986. One source estimated that 10% of all the PCs in the Gulf Emirates were affected by the virus, which writes garbage into the BIOS and can erase hard drives.

Date 1999-05-03 **Keyword** virus creator law enforcement plaintiffs hacker

Source, Vol, No. Australian Financial Review

Although 24-year-old Taiwanese information technologist Chen Ing-hau admitted writing the Chernobyl virus (also called CIH, the authors initials), local prosecutors were unable to charge him with anything because no one local had complained about the virus. Mr Chen apologized for the damage caused to hundreds of thousands of computers in Bangladesh, China, India, South Korea, Turkey, and many other countries with poor anti-virus precautions in place.

Date 1999-05-11 **Keyword** virus Trojan e-mail

Source, Vol, No. South China Morning Post (Hong Kong)

In May 1999, reports surfaced of a Chinese Trojan called picture.exe that had been circulating widely in China since December 1998. The program, also known as manager.exe, was circulated via an e-mail vector and would send infected-system configuration data to e-mail addresses in the PRC.

Date 1999-05-28 **Keyword** Trojan back door malicious code spam attachment

Source, Vol, No. MSNBC

Network Associates Inc. anti-virus labs warned of a new Trojan called BackDoor-G being sent around the Net as spam in May. Users were tricked into installing "screen savers" that were nothing of the sort. The Trojan resembled the previous year's Back Orifice program in providing remote administration -- and back doors for criminals to infiltrate a system. A variant called "Armageddon" appeared within days in France.

Date 1999-06-11 **Keyword** virus e-mail attachment Windows worm executable

Source, Vol, No. Wall Street Journal

The Worm.Explore.Zip (aka "Trojan Explore.Zip) worm appeared in June as an attachment to e-mail masquerading as an innocuous compressed WinZIP file. The executable file used the icon from WinZIP to fool people into double-clicking it, at which time it began destroying files on disk. Within a week of its discovery in Israel on the 6th of June the worm had spread to more than 12 countries. Network Associates reported that ~70% of its largest 500 corporate customers were infected. [Readers should remember that the larger the number of computers in a company, the more likely that at least one will be infected even when infection rates are low. If the probability of infecting one system is "p" and there are "n" targets in a group each of which can be infected independently, the likelihood of at least one infection in the group is P = {1 - (1 - p)^n} which rises rapidly as n increases.]

Date 1999-07-12 **Keyword** criminal hacker penetration tool Trojan version WindowsNT

Source, Vol, No. AP

The Cult of the Dead Cow released BackOrifice 2K (B02K), the newest version of its 1998 penetration tool, BackOrifice (named as a lampoon of the BackOffice product of Microsoft). BO2K, usually installed illegally on victim machines through a contaminated vector program that has been thereby transformed into a Trojan horse, allows complete remote control and monitoring of the infected PCs. BO2K was noteworthy because it attacks WindowsNT workstations and servers and thus has even more serious implications for INFOSEC. Anti-virus companies worked feverishly immediately after the release of the tool to update their virus-signature files. A criminal hacker calling himself Deth Veggie insisted that the CDC is involved in guerilla quality assurance — their penetration tools, he argued, would force Microsoft to repair the "fundamentally broken" Windows operating systems. Jason Garms, lead product manager for Windows NT security, disagreed strongly: "I certainly categorize what they're trying to do as being malicious. This program they have created has absolutely no purpose except to damage users." He added, "You can't walk down the street and pick up a rock and throw it through someone's window. You'd be arrested. But there are people on the Internet that would argue that it's good behavior because that window should have been stronger. In the real world you can't say 'You should have bulletproof glass on your windows."

Date 1999-07-12 **Keyword** criminal hacker remote control penetration Trojan tools

Source, Vol, No. Canberra Times (Australia)

David Hellaby of the Canberra Times (Australia) published a good review of remote-control software used by criminal hackers. Some of the dangerous applications are BackOrifice, BackOrifice 2000, DeepThroat 1, 2 and 3, EvilFTP, ExploreZip.worm, GateCrasher 1.2, GirlFriend 1.3, Hack'a'Tack, NetSphere 1.30,phAse Zero, Portal of Doom, and SubSeven (aka BackDoor-G). These programs are usually integrated into otherwise harmless and useful vector programs to create Trojans that are downloaded from the Net or shared among hapless victims. Symptoms of remote control sound like a nightmare from a paranoid schizophrenic's worst crisis: "your CD draw begins opening and closing, your web browser starts on its own, strange messages appear on your screen, and your PC seems to be haunted." The author warned his readers to be very careful about opening attachments to e-mail messages.

Date 1999-08-19 **Keyword** virus payload latency trigger logic bomb Windows operating systems

Source, Vol, No. Wall Street Journal

The Command anti-virus company announced discovery of the Win32.Kriz.3862 virus, which runs successfully under Windows 95, 98 and NT. This logic bomb would detonate on Christmas day; its payload includes massive overwriting of data on all data storage units and also damage to the BIOS. However, the virus had not been found outside the lab and so would be a low to medium risk, according to the researchers.

Date 1999-09-02 **Keyword** Word 97 macro virus

Source, Vol, No. PC Week Online, Computerworld <

In mid-August, Symantec announced discovery of a dangerous MS-Word 97 macro virus called "Thursday" with a trigger date of 13 Dec. The virus turns off macro warnings in MS-Word. This virus was seen in the wild on about 5,000 computers in Austria, France, Germany, Ireland, Latvia, Poland, Switzerland, the UK, and the US. The payload can erase all files on the C: drive. All major anti-virus companies issues updates to their signature files to catch this virus.

Date 1999-09-09 **Keyword** virus macro worm

Source, Vol, No. PC World Online

Computer Associates International discovered a dangerous new virus/worm called Cholera. This laboratory virus sent itself through e-mail attachments to all available e-mail addresses found on a MAPI-compliant system. The virus/worm sent a message with a smiley face symbol and an attachment called "setup.exe" which foolish users might execute. The virus portion would then load itself into memory and insert software keys into WIN.INI and the Windows 9x registry file.

Date 1999-09-20 **Keyword** virus worm Trojan e-mail Y2K countdown clock fix Internet passwords

Source, Vol, No. San Francisco Chronicle

A couple of new Y2K-related virus/worms were discovered in September. One e-mail Trojan called "Y2Kcount.exe" claimed that its attachment was a Y2K-countdown clock; actually it also sent user IDs and passwords out into the Net by e-mail. Microsoft reported finding eight different versions of the e-mail in circulation on the Net. The other, named "W32/Fix2001" came as an attachment ostensibly from the system administrator and urged the victims to install the "fix" to prevent Internet problems around the Y2K transition. Actually, the virus/worm would replicate through attachments to all outbound e-mail messages from the infected system. [These malicious programs are called "virus/worms" because they integrate into the operating system (i.e., they are virus-like) but also replicate through networks via e-mail (i.e., they are worm-like).]

Date 1999-10-11 **Keyword** virus WindowsNT TSR terminate-stay-resident

Source, Vol, No. Network World Online

The WinNT.Infis virus was the first NT-specific virus found in the wild (in Russia). The virus was described as having a novel stealth mechanism.

Date 1999-11-01 **Keyword** free anti-virus software Microsoft Y2K preparations

Source, Vol, No. InfoWorld Electric, Microsoft < www.microsoft.com/y2k >

Microsoft contracted with nine anti-virus product vendors to distribute their software free on its Web site. The move was described as preparation for particularly heavy virus attacks during the Y2K transition. Participants included Central Command, Computer Associates, Data Fellows, Network Associates, Norman ASA, Panda Software, Sophos, Symantec and Trend Micro.

Date 1999-11-10 **Keyword** virus worm e-mail attachment highlight automatic MS-Outlook prototype proof-of-concept

Source, Vol, No. AP, Dow Jones

In early November, a worrisome new worm appeared on the scene. The BubbleBoy proof-of-concept worm was sent to Network Associates, who immediately posted a free software patch and alerted the FBI of the danger. The problem with this worm was that it would infect a host if an MS-Outlook user merely highlighted the subject line of the carrier e-mail message -- no double-clicking required. The worm's payload was mild -- changes to the registry and a simple display screen -- but experts warned that the same techniques could carry much more dangerous payloads in future variations. The worm spread by mailing itself to every e-mail address on the infected system's address list, thus posing an even greater potential danger than the Melissa worm. [This attack again demonstrates the foolishness of allowing automatic execution of code by e-mail and word-processing packages.]

Date 1999-11-12 **Keyword** virus Windows NT patch security kernel

Source, Vol, No. Newsbytes

The W32.FunLove.4099 virus discovered by the Symantec AntiVirus Research Center (SARC) in November, attacks Windows NT in a new way: by patching the security kernel. The virus modifies file access so that all files are accessible to any user — a perfect setup to allow a criminal hacker to wreak havoc on an infected system.

Date 1999-11-19 **Keyword** criminal hacker attitude stance belief anti-virus malicious code definitions criteria

Source, Vol, No. HackCanada

Someone calling itself "Renderman" at HackCanada raised a legitimate question about the criteria used to define software as malicious by anti-virus product developers. This issue was the subject in early 1999 of a working group at the European Institute for Computer Anti-Virus Research (EICAR), which concluded that trying to integrate the motivation behind a program was a hopeless basis for defining malware.

Date 1999-11-19 **Keyword** virus damage cost production factory

Source, Vol, No. Reuters

Dell Computer's plant in Cork, Ireland suffered five days of downtime after the company discovered that 500 of its computers had been infected with the FunLove virus. Staff had to track down the source of the infection and eradicate the virus from all its systems. Paul Taylor (Reuters) wrote, "the attack is regarded as one of the most damaging seen in Europe." In addition to the lost production time, the incident damaged customer relations, with some customers complaining about the delay in delivery of their systems.

Date 1999-11-23 **Keyword** anti-virus screening network Web ISP Internet service provider central server

Source, Vol, No. Newsbytes

US West announced that its 25M Internet customers would be shielded by Trend Micro's InterScan Virus Wall, and low-cost ($24.95) copies of Trend Micro's PC-cillin for the desktop. The $1.50/month service, said the firm, would reliably block e-mail-borne viruses and worms.

Date 1999-12-02 **Keyword** virus worm e-mail attachment Trojan misleading subject automatic excecution double-click open

Source, Vol, No. DOW JONES BUSINESS NEWS; Australian

At the end of November, anti-virus experts reported a flurry of infections by the Mini-Zip e-mail enabled virus/worm, a variant of the Worm.ExploreZip virus that appeared in June. This virus/worm was compressed, so it was not recognized using the known signature strings for the original virus/worm. Once resident, the Mini-Zip program reads the addresses of new e-mail in MS-Outlook and automatically sends itself as a responseusing the "RE: " convention. The fraudulent message text is, "Hi <recipient-name>! I received your e-mail and I shall send you an e-mail ASAP. Till then, take a look at the attached zipped docs. bye." However, the attachment is actually a dropper program that installs the viral code in memory on Windows 9x and Windows NT systems and continues the spread of the attachment through e-mail. In addition, the virus code resets file lengths on the C: drive to zero, causing major damage and making it hard to recover files on the damaged disk.

In December, more than 120 of Australia's largest companies were hit by the virus, causing two days of downtime. Reports that Compaq Australia may have been the first Australian site hit by the virus and therefore responsible for sending out infected e-mail caused embarrassment to that company.

Date 1999-12-03 **Keyword** virus worm BIOS checksum Y2K new year trigger date format hard drive boot error message

Source, Vol, No. Dow Jones, Computerworld <http://www.computerworld.com/home/news.nsf/all/9912035y2kworm

The upsurge in e-mail-enabled worms and viruses in late 1999 supported the predictions of anti-virus experts who said that the Y2K transition would see a flurry of new viruses and variants that would contribute to confusion about the source of software problems following New Year's Day 2000.

Nancy Weil, writing in ComputerWorld <http://www.computerworld.com/home/news.nsf/all/9912035y2kworm>, suggested that the Worm.Mypic (aka W32/Mypics.worm) identified in the first days of December demonstrated the kind of problem we were to face in the following weeks. Worm.Mypic arrives as an executable attachment (Pics4You.exe with a length of 34,304 b). If executed, the program e-mails itself to the usual first 50 names in the MS-Outlook address list (and continues to try to do so at regular intervals). As soon as the date changes to 1 Jan 2000, the resident virus overwrites checksum data for the computer's BIOS, interfering with the boot sequence. The virus also attempts to format C: and D: drives.

As usual, everyone agreed that it was critically important to update virus-signature files even more freqently than usual as we approached the new year.

Date 1999-12-04 **Keyword** anti-virus server e-mail content filtering screening

Source, Vol, No. Computer Reseller News

Amy Rogers of Computer Reseller News pointed out in her December 4th article that several companies have been quick to develop server-based e-mail content-filtering software to fight the growing threat of e-mail-enabled viruses and worms. Examples include Finjan, TenFour and Worldtalk.

Date 1999-12-07 **Keyword** virus Trojan

Source, Vol, No. PR Newswire

Computer Associates issued a warning about the W.95.Babylonia virus, described as an extensible virus whose payload could be modified remotely by its author. The December outbreak of Babylonia in the wild involved a Trojan disguised as a Y2K bug fix for Internet Relay Chat (IRC) users. The Trojan would send itself to other users and also poll an Internet site in Japan looking for updated plugins to alter the effects of the malicious software.

Date 1999-12-08 **Keyword** virus overview

Source, Vol, No. Age (Melbourne, Australia)

Computer Associates (Australia) reported a major rise in damage from a rash of new and increasingly virulent viruses. Apparently one of the most serious viruses in Australia was W32/Mypics.

Date 1999-12-10 **Keyword** virus worm e-mail denial-of-service crash attachment police

Source, Vol, No. News wires, ZDNet < http://dailynews.yahoo.com/h/zd/19991210/tc/19991210060.html >

The search for the originator of the Melissa e-mail computer virus began immediately after the outbreak. Initial findings traced the virus to Access Orlando, a Florida ISP, whose servers were shut down by order of the FBI for forensic examination; the systems were then confiscated. That occurrence was then traced back to Source of Kaos, a free-speech Web site where the virus may have lain dormant for months in a closed but not deleted virus-distributor's pages. In an interesting wrinkle, the MS-Word serial number on the original infected documents were circulated on the Net to help track down the perpetrator. The next steps turned to AOL, where the virus was released to the public. The giant ISP's information named a possible suspect and by the 2nd of April, the FBI arrested David L. Smith (aged 30) of Aberdeen, NJ. Smith apparently panicked when he heard the FBI were on the trail of the Melissa spawner and he threw away his computer -- stupidly, into the trash at his own apartment building. Smith was charged with second degree offenses of interruption of public communication, conspiracy to commit the offense and attempt to commit the offense, third degree theft of computer service, and third degree damage or wrongful access to computer systems. If convicted, Smith faced a maximum penalty of 480,000 dollars in fines and 40 years in prison. On 10 December, Smith pleaded guilty to all federal charges and agreed to every particular of the indictment, including the ICSA.net estimates of at least $80M of consequential damages due to the Melissa infections.

Category 15 Fraud (not embezzlement), extortion, slamming

Date 1999-02-03 **Keyword** Internet credit repair fraud FTC crackdown lawsuits scam

Source, Vol, No. Wired via PointCast

The FTC and 14 state Attorneys General launched aggressive lawsuits against three credit-repair agencies that taught people with bad credit histories to lie their way to a new credit history. The dishonest victims of the fraudsters paid U$22-$40 to learn techniques for fraud. According to an article for Wired written by Heidi Kriz, credit-repair fraud instructions are the ninth most popular criminality on the Web today. Quoting Cleo Manuel of the Internet Fraud Watch consumer-protection organization, the author noted that the number one Internet fraud today is online auctions. [Comment from MK: online gambling involving unverifiable results of a game or in online auctions involving unverifiable bids by possibly virtual bidders constitute a tax on low IQ.]

Date 1999-02-15 **Keyword** online auctions theft fraud misrepresentation court case law

Source, Vol, No. USA Today

The online eBay auction house was embarrassed when someone offered computers for sale via its services, collected money for the items and then defaulted on delivery. The malefactor was convicted of fraud in federal court in mid-February.

Date 1999-02-23 **Keyword** Internet fraud scam FTC online consumers survey study statistics

Source, Vol, No. AP, UPI

The National Consumers League's Internet Fraud Watch received 7,752 complaints about Internet-based fraud in 1998 compared with 1,280 in 1997. In February, the Federal Trade Commission announced it would institute a 24-hour fraud-detection service in March 1999. Internet Fraud Watch reported that the top 10 complaints were (in order of frequency): auctions, general merchandise sales, computer equipment and software, Internet services, work-at-home offers, business opportunities, marketing schemes, credit card offers, advance fee loans and employment offers.

Date 1999-03-01 **Keyword** credit card fraud prevention profiling

Source, Vol, No. RISKS 20 23

A diner's credit card was refused because (1) he and his wife had bought expensive tableware that was charged in two lots at the store; (2) the credit-card company's profile of habitual purchase patterns was tripped by the unusual pattern; (3) a hold was put on the credit card; and (4) no one bothered to inform the user. [Moral: if you're going to impose security profiles on a system, you have to follow through all the way. Half a security measure can be worse than none.]

Date 1999-04-08 **Keyword** fraud Internet auction eBay FBI investigation

Source, Vol, No. CNET news.com, Reuters

The integrity of Web-based auctions has been questioned before, but in February the eBay auction-house admitted that the FBI and the New York State Department of consumer affairs were investigating the practices of some of its sellers. Problems included sales of guns to unauthorized buyers and sales of illegally copied software. The company was also accused of failing to make it clear to buyers that it takes no responsibility for completion of the transactions initiated through its service nor for quality or deliver of goods sold online. In April, the firm settled with the NY regulators on a plan for cracking down on fake sports memorabilia sold through its service.

Date 1999-04-16 **Keyword** fraud securities Web forgery insider trading stock

Source, Vol, No. CNN

Gary Dale Hoke was arrested by the FBI for allegedly creating a bogus Web page that simulated the Bloomberg information service and touted Pairgain stock as undervalued because of an impending takeover; the false information deceived investors into bidding up the price of Pairgain stock, causing windfall gains for some stockholders and losses for others when the price fell back to normal. The accused faces fines in the $M and up to 10 years in jail for stock manipulation. The FBI tracked the perpetrator using cooperation from ISPs and access to their Internet server log files.

Date 1999-04-21 **Keyword** fraud credulity irresponsible press lies massacre shooting

Source, Vol, No. AP

People with a sick sense of humor posted fraudulent ex post facto "warnings" about the Littleton, Colorado High School attack in several AOL member profiles.

Date 1999-04-23 **Keyword** privacy Web Internet detectives private investigators fraud

Source, Vol, No. New York Times

The FTC announced that it would crack down on private investigators using deceit to obtain confidential information. FTC charged James and Regina Rapp, who advertised on the Web that their company, Touch Tone Information, could obtain private data such as bank records and unlisted phone numbers. The Rapps admitted to instructing employees to make hundreds of phone calls under false pretences--banned by the Federal Trade Commission Act. James Rapp shut down his Web site and promised to stop lying to get information but claimed that such limitations on his practice would only hurt victims. Sneered Rapp, "If you're a dead-beat dad or a neglected spouse you don't have to worry anymore." [The New York Times did not report on Mr Rapp's explanation of why bad people could not equally well use his service for nefarious purposes.]

Date 1999-04-26 **Keyword** fraud scam thieves Y2K gullible victims banks PCs software

Source, Vol, No. AP

Criminals have been taking advantage of the Y2K frenzy by selling electronic snake-oil: magical programs that fix Y2K problems instantly and without effort. Others are not even bothering with the product: they sell stocks in their fraudulent corporations by claiming to have vague but wonderful products that will sell madly in the last quarter of 1999. People have been tricked into moving their bank deposits into "another" bank account as part of their bank's Y2K efforts -- only to discover that the other bank account belonged to someone else who has cleared it out and disappeared.

Date 1999-05-07 **Keyword** privacy children commerce Internet Web law government FTC

Source, Vol, No. AP

The FTC and Liberty Financial Companies arrived at a settlement after the company misled visitors to its "Young Investor" Web site by claiming that survey data would be "kept anonymous." In fact the company gathered personal details including name and e-mail address and sent advertising to its visitors. In addition, said the FTC, the company enticed children into filling out detailed surveys by promising prizes but the company never actually selected winners for the prizes or sent out the newsletters. Company spokesperson claimed that this was "an administrative error" and hurriedly arranged to award their prizes.

Date 1999-05-11 **Keyword** Internet Web fraud organization e-commerce crime

Source, Vol, No. Reuters

In May, the new Internet Fraud Council started work on standards for Internet businesses to help fight fraud. They proposed a clearinghouse to share information about different types of fraud on the Net and announced that they would collaborate with law enforcement initiatives to quash fraud.

Date 1999-07-15 **Keyword** fraud online auction eBay investigation court case prosecution guilty

Source, Vol, No. CNET news.com <http://news.cnet.com/category/0-1007-200-344903.html>

Robert Guest of Los Angeles admitted in court in July that he defrauded victims of around $37,000 by offering goods for auction via eBay but failing to deliver anything.

Date 1999-09-03 **Keyword** fraud online auction e-commerce hoax kidney organs

Source, Vol, No. CNET news.com <http://news.cnet.com/category/0-1007-200-346765.html>

In September, someone put up a human kidney for sale through the online auction-house eBay and received bids of up to $5.8M. The auction service canceled the sale because selling human organs is a Federal felony with up to $250,000 in fines and at least 5 years in jail.

Date 1999-09-07 **Keyword** online auction traffic human baby unborn fetus eBay

Source, Vol, No. CNET news.com n<http://news.cnet.com/news/0-1007-200-346836.html>

A week after someone claimed to want to sell a human kidney online, eBay had to shut down an auction for an unborn human baby. Prices for the supposed baby had risen into the $100K range before eBay pulled the plug.

Date 1999-09-23 **Keyword** fraud online auction drug marijuana dope traffic

Source, Vol, No. CNET news.com <http://news.cnet.com/category/0-1007-200-123002.html>

Someone tried to sell 500 pounds of fresh marijuana via online auction-house eBay. The auction was shut down after 21 hours, during which prices offered had reached $10M.

Date 1999-10-12 **Keyword** fraud Internet e-commerce spam study statistics survey

Source, Vol, No. CNET news.com

The incidence of fraud through online sales and auctions is increasing as the volume of these transactions increases. Troy Wolverston and Greg Sandoval interviewed several experts on computer crime for CNET news.com and found a consensus that easy anonymity is at the root of easy crime.

Date 1999-10-15 **Keyword** indictment extortion teenager threats bomb Internet

Source, Vol, No. AP via Las Vegas Sun <http://www.lasvegassun.com/sunbin/stories/text/1999/oct/15/101500270.ht

Jahair Joel Navarro, an 18-year-old from New York state, was indicted in White Plains on charges of extortion. He allegedly threatened to bomb Microsoft and IBM headquarters unless each company paid him $5M. An FBI raid on the lad's apartment found no bombs but only the usual instructions on bomb-making downloaded from the Internet.

Date 1999-11-15 **Keyword** fraud scam information warfare stock price manipulation securities

Source, Vol, No. The Times (London)

Investors in the USA and in the UK were warned off "pump-and-dump" frauds in which false information is used to generate interest in stocks. Typically the fraudsters buy cheap and then try to move the share price higher by posting exciting but wrong news about the company's prospects. Cases have involved losses in the millions of dollars. One of the techniques used by the criminals is to put up Web sites that resemble or even duplicate those of the real company and link to them from their own bogus sites.

Date 1999-11-16 **Keyword** Internet Web fraud bogus prosecution

Source, Vol, No. Reuters

The New Jersey Attorney General charged nine people on several complaints of fraud from 1996 through 1998. Some of the scams included selling non-existent stock for $850,000, selling non-existent Beanie Babies through the eBay online auction service, and selling Viagra through the Net without a license.

Category 16 INFOWAR, industrial espionage,

Date 1999-01-04 **Keyword** criminal hackers industrial espionage software piracy theft

Source, Vol, No. Reuters

Unemployed Russian computer programmers pose a serious threat to world computing, according to Elizabeth Piper, writing for Reuters. With 89% of all the programs in Russia being pirated, the habits are well inculcated already; however, the growing economic crisis is throwing programmers into desperation. Many are turning to hacking, including industrial espionage, to make a living.

Date 1999-01-04 **Keyword** information warfare strategy national security

Source, Vol, No. Federal Computer Week <http://www.fcw.com/pubs/fcw/1999/0104/web-rand-01-04-98.html>

The RAND Corporation issued a DoD-commissioned report, "Strategic Information Warfare Rising" in mid-1998 that fueled the growing debate within the Pentagon about the wisdom of pursuing offensive information warfare capabilities. Opponents argue that widening the sphere of warfare to include cyberattacks on critical infrastructure would only increase likelihood of successful attacks on the US. The report laid out four basic scenarios for future developments in IW; as laid out by Daniel Verton, writing in Federal Computer Week, they were the following [bullets added]:
"* U.S. supremacy in offense and defensive strategic IW.
* A club of strategic IW elites, whereby a policy of no first use of strategic IW capabilities could be established.
* Global "defensive dominance" in strategic IW, whereby a regime would be established to control the spread of strategic IW similar to biological and chemical weapons.
* Market-based diversity, whereby the damage or disruption achievable through a strategic IW attack is modest and recovery is fast."

Date 1999-01-08 **Keyword** network defense information warfare INFOWAR criminal hackers spies DoD

Source, Vol, No. UPI, OTC

The Joint Task Force - Computer Network Defense (JTC-CND) was announced on 1999-12-08 and officially launched on the 1999-01-01. The JTC-CND immediately generated controversy among politicians and industry security experts who argued that the agency should concentrate on proactive identification of vulnerabilities and measures to plug the security holes. In contrast, spokespeople for the Task Force seemed to emphasize a more reactive approach, where they would respond to cyberattack in real time. Melissa Bohan, speaking for the office of USAF Maj. Gen. John Campbell, the new head of the task force, said that detecting intrusions was a primary function; "Who may have made that intrusion is often a secondary question. In fact, 'who' it is may not even be important." By August 1999, the JTF-CND was fully operational and monitoring Pentagon networks for intrusions round the clock.

Date 1999-01-29 **Keyword** government support education infrastructure scholarships

Source, Vol, No. Science

The Clinton administration proposed a 40% increase in critical infrastructure protection and computer security -- a proposed budget item of $1.464B. Some $3M of this amount was earmarked for new scholarships in computer science and security programs.

Date 1999-02-12 **Keyword** sabotage information warfare knowbot feedback fraud error

Source, Vol, No. RISKS 20 21

For unknown reasons, the BUY.COM online store Web site listed a $588 Hitachi monitor at only $164.50 -- and staff failed to notice the error until two days later, by which time there were 1,600 orders for this incredible bargain. The potential cost in lost revenue was $677,600 and the real cost depended on the markup. Analysts speculated on the cause of the error. One intriguing possibility: the BUY.COM online store has a policy of underbidding any price on the Net and may possibly use knowbots to scour the Web looking for prices of products it sells. If a competitor accidentally or deliberately posted a bad price, the unsupervised knowbot could very well poison the Web site database. The same technique could be used in an information warfare attack to ruin a competitor.

Date 1999-02-16 **Keyword** pentagon information warfare data leakage inference Web

Source, Vol, No. AP

The Pentagon began a thorough re-evaluation of the value of its public Web sites after information warfare experts demonstrated in December 1998 that open-source information could be used to infer sensitive information such as the location of military personnel's family members. Before the purge, tactically valuable data such as aerial reconnaissance photographs showing US military installations were freely available to anyone, including terrorists.

Date 1999-02-18 **Keyword** information warfare critical infrastructure protection

Source, Vol, No. COMPUTING (UK)

Colin Barker wrote an interesting essay on the change in the British government's attitude towards information warfare. In February, the UK announced that there would be a one-day conference entitled Protecting the National Information Infrastructure. Barker attributes the change in part to the effect of the Y2K bug on non-technical politicians and bureaucrats. First, the bug brought home just how dependent modern society is on computer and networks; second, it raised doubts about the competence of the I.T. specialists who had been denying that information warfare was a serious issue.

Date 1999-02-25 **Keyword** information warfare infrastructure vulnerability government

Source, Vol, No. Computing (UK)

In February, the largest information warfare conference in Britain was organized by the UK government's information security branch, the Communications Electronics Security Group (CESG). The conference was mostly held away from the public and press, but analysts suggested that the key issue was critical infrastructure protection in the face of increasing threats from criminals, ideologues, hobbyists and agents of international antagonists -- governmental and terrorist.

Date 1999-02-28 **Keyword** criminal hacking interception industrial sabotage infowar

Source, Vol, No. Reuteurs; RISKS

In late February, the Sunday Business newspaper quoted an unnamed source that claimed that criminal hackers had achieved control over a British communications satellite and were making extortion threats. The story was later discredited.

Date 1999-03-01 **Keyword** information warfare international crime fraud pornography

Source, Vol, No. Washington Post

Janet Reno, the Attorney General of the U.S., announced the formation of a center for fighting Internet-based computer crime. She also called for international cooperation and laws to fight cybercrime.

Date 1999-03-30 **Keyword** information warfare Web vandalism hacktivism denial

Source, Vol, No. BBC, news wires

Serbian hackers began a low-level campaign of harassment directed at US government and military agencies as NATO began bombing Serbia in March 1999. The "Black Hand" hacker group, possibly named after the notorious Sicilian secret society associated with the Mafia, and the "Serbian Angel" hackers threatened to damage NATO computers in retaliation for the war against the Serbs. The White house Web site was defaced by red letters reading "Hackerz wuz Here" on the 29th of March. Speculation was rife that anti-NATO activists were involved. According to a Russian newspaper, "Segodyna," on the 30th of March, unknown hackers damaged a main NATO Web server; the system was down for at least half an hour. The claim was unconfirmed by NATO sources.

Date 1999-04-03 **Keyword** information warfare Web vandalism hacktivism

Source, Vol, No. LOS ANGELES TIMES 03/04/1999 P10

The Kosovo conflict generated a flurry of hacking in what the media labeled the "First Internet War," the "First CyberWar" or the "Web War I." Serbs and Albanians and their supporters attacked each others' Web sites — and those of NATO — leaving messages such as "If you're looking for the truth, visit WWW.B92.NET," and the ever-popular and eternally misspelled, "SAMURAI RULLEZ!"

Date 1999-04-04 **Keyword** information warfare survey estimates virus damage costs

Source, Vol, No. SUNDAY TIMES

A report in the Sunday Times reviewed the growing scope and cost of information warfare around the world. New e-mail-enabled viruses and new Trojans have the potential for massive damage running into the billions of dollars, according to experts such as CSI's Richard Power. James Adams, of Infrastructure Defence and author of _The Next World War: Computers are the Weapons and the Front Line is Everywhere_, said, "Hackers are a new form of terrorist. You can bring a country to its knees. It is a unique weapon. Things are getting exponentially worse."

Date 1999-04-04 **Keyword** information warfare vandalism Web Internet

Source, Vol, No. Sunday Times (London), Defense Daily

The British GCHQ warned in April 1999 that Serbian hackers might see infrastructure systems as prime targets for electronic attack given the perceived difficulty of penetrating government and military computers. The US DoD stated in June 1999 that Serb hackers were definitely probing Pentagon systems but had not succeeded in penetrating any.

Date 1999-04-06 **Keyword** information warfare Web vandalism hacktivism

Source, Vol, No. OTC

As the incidence of information warfare attacks grew during the Kosovo conflict, some security firms found their business going up. Internet Security Systems of Atlanta got a contract with the US Army and the Air Force for security improvements to their Web sites.

Date 1999-04-09 **Keyword** information warfare espionage propaganda Web attack

Source, Vol, No. BBC MONITORING SERVICE: CENTRAL EUROPE & BALKANS

The government of Serbia claimed that the CIA hijacked their Web site but said in April that everything was OK now.

Date 1999-04-19 **Keyword** information warfare attacks cyberwar Netwar NATO

Source, Vol, No. mi2g PR

The mi2g security group based in London, England claimed that pro-Serbian cyberwarriors were sending virus-laden e-mail to various businesses, hospitals, and government agencies throughout NATO countries in a concerted effort to cause disruption during the Kosovo air-war launched against Serbia by NATO.

Date 1999-04-20 **Keyword** information warfare cyberwar Netwar strategy terrorists

Source, Vol, No. Wired

An interesting paper by the Rand Corporation entitled _Countering the New Terrorism_ was put on the Web free < http://www.rand.org/publications/MR/MR989/MR989.pdf >. _Countering the New Terrorism_ by I.O. Lesser, B. Hoffman, J. Arquilla, D.F. Ronfeldt, M. Zanini, & B.M. Jenkins was abstracted as follows: "The contours of terrorism are changing, and the new terrorism has more diverse sources, motivations, and tactics than the old. It is more lethal, global in reach, and characterized by network forms of organization. Terrorist sponsorship is becoming hazier and `privatized.' The August 1998 terrorist bombings of U.S. embassies in Kenya and Tanzania fit in many ways the new mold. The chapters in this book trace the evolution of international terrorism against civilian and U.S. military targets, look ahead to where terrorism is going, and assess how it might be contained. Terrorism and counterterrorism are placed in strategic perspective, including how terrorism might be applied as an asymmetric strategy by less-capable adversaries. The report builds on a existing body of RAND research on terrorism and political violence, and makes extensive use of the RAND-St. Andrews Chronology of International Terrorism."

Date 1999-05-09 **Keyword** hacktivists political protest Web government China USA Belgrade embassy bombing

Source, Vol, No. ABC <http://www.abcnews.go.com/sections/world/DailyNews/kosovo_chinacyber_990509.html >,

In the wake of the US bombing of the Chinese embassy in Belgrade, hactivists assaulted a number of US Web sites and launched a propaganda offensive on chat boards. Damaged Web sites included those of the US Embassy in China, the Department of Energy, the Department of the Interior, and the Department of Energy.

Date 1999-05-24 **Keyword** information warfare INFOWAR destablize government secret attack hacking

Source, Vol, No. Newsweek via Reuters

Newsweek Magazine claimed in May 1999 that the Clinton Administration had agreed to attack the Milosevic regime in Yugoslavia using information warfare techniques such as damaging the dictator's foreign bank accounts and carrying out sabotage within his country to foment dissatisfaction. The anonymous sources claimed that the CIA would be involved, but equally anonymous sources denied this assertion.

Date 1999-06-02 **Keyword** information warfare criminal hackers vandalism espionage air gap

Source, Vol, No. Washington Post

In June, the Pentagon installed firewalls between sensitive and less-sensitive components of its networks. Some observers interpreted this move as a response to highly-publicized successful attacks on DoD sites by criminal hackers in the preceding months.

Date 1999-09-30 **Keyword** information warfare strategy planning theory commercial off-the-shelf software COTS infrastruct

Source, Vol, No. Defense Daily 203 64

Marvin Langston, Deputy Assistant Secretary of Defense (C3I) and the Office of the Secretary of Defense's Deputy Chief Information Officer, told a National Defense University group in September that the Pentagon needs to put more effort into defensive and offensive information technology. He also warned that the DoD's dependence on commercial off-the-shelf software (COTS) makes it impossible to achieve information superiority; the DoD, he concluded, must invest in much more research and development for its particular technological needs.

Date 1999-10-01 **Keyword** information warfare infowar criminal hacker attack penetration vandalism hacktivism law enforce

Source, Vol, No. Defense Information and Electronics Report

James Christy of the Defense-wide Information Assurance Program (DIAP) offered a strongly-worded attack on the notion that the US has ever been the target of information warfare. On the contrary, he argued in a presentation to the International Testing and Evaluation Symposium in Atlanta in late September, the attackers are cybercriminals, not cyberwarriors. The fundamental difficulties in responding effectively to such attacks, said Christy, are as follows:
* the military has expertise in computer crime but cannot help law enforcement agencies without a presidential directive;
* the civilian has not been able sufficiently to develop its familiarity with computer crime countermeasures;
* it is difficult to tell that cyberattacks are being carried out because most victims keep that information secret, not wanting to get involved with law enforcement investigators;
* precise attribution of blame is extremely difficult in cyberspace;
* the public doesn't know much about computer crime and therefore tends to favor privacy over cybercrime prevention and law enforcement;
* jurisdiction over cyberspace crimes is confused by competing geographical claims.

Date 1999-10-04 **Keyword** information warfare foreign penetration attempts attacks firewalls defenses

Source, Vol, No. Dow Jones International newswires, Australian AP

Richard Humphrey, Managing Director of the Australian Stock Exchange, claimed in an interview that a foreign military site attacked the Exchange in late 1998. He implied that the site was in the USA, although apparently the "foreign" military officials who were contacted denied any possibility of such an attack from a military site. Humphrey urged changes in Australian laws to make it easier to try hackers; at present the laws require that criminal hackers be apprehended in the act of hacking.

Date 1999-11-11 **Keyword** information warfare espionage criminal hacking civil lawsuit

Source, Vol, No. PR Newswire

In the first case of a lawsuit involving industrial espionage by lawyers, Moore Publishing of Wilmington, DE sued Steptoe & Johnson of Washington, DC for allegedly breaking into its computer systems more than 750 times while simultaneously using a stolen user-ID and password to penetrate the victim's network. In addition, the suit alleges a systematic cyberwar involving misinformation posted on newsgroups through a HotMail account that was eventually traced to the defendants. The suit demanded damages of at least $10M.

Date 1999-11-17 **Keyword** information warfare infrastructure vulnerability national defense

Source, Vol, No. AAP

Australian Attorney-General Daryl Williams gave a clear warning on November 17th about the necessity for infrastructure protection in the era of cyberwar. Speaking at the Security in Government Conference, he said, "Australia's security is open to compromise in ways that may be less obvious than a terrorist attack but are certainly no less significant." The Attorney-General added, "The costs of a deliberate and concerted attack on our telecommunications, energy, banking and finance or air traffic control systems would be immense in both social and financial terms. The potential sources of deliberate threats are familiar to us all: disgruntled employees or contractors, criminals, issue-motivated groups, terrorists, those engaged in commercial espionage and some foreign states. As if these are not enough, there are also new villains on the scene. The computer hacker and cyber terrorist, sometimes operating alone and equipped only with a personal computer and a modem, can inflict the kind of damage that was previously the realm of organised well-resourced groups." He urged cooperation between the government and the private sector and suggested that a vulnerability and threats database would be useful.

Date 1999-11-17 **Keyword** information warfare doctrine review survey study analysis

Source, Vol, No. Jiefangjun Bao (Beijing) translated by BBC

The Chinese military newspaper Jiefangjun Bao published an article in November emphasizing the importance of information warfare in the current military sphere. The authors, Leng Binglin, Wang Ylin and Zhao Wenxiang, made the tendentious claim that "In the Kosovo war, the Yugoslav Federation organized a `hacking' war to attack certain US, British, and NATO web sites, which forced the White House and Pentagon computer systems to cease operations, while the British Meteorological Office was paralysed and unable to provide the necessary meteorological services for NATO air attacks, and a number of NATO air attack plans even had to be cancelled." The concluded, "Experts concerned believe that net attacks have not yet been fully put to good use, because corresponding links have not been established between such attacks and combat actions, since each fights its own war. To ensure that net warfare can play the maximum role in war, it is essential to integrate it with other combat actions. Modern hi-tech warfare cannot win without the net, nor can it be won just on the net. In the future there must be coordinated land, sea, air, space, electronic, and net warfare, and the state's determination will be fully expressed in this mysterious theatre space." [The article was particularly interesting because of the ongoing cyberwar waged by Taiwan and The People's Republic in which there have been thousands of attacks on each others' Web sites.]

Date 1999-11-18 **Keyword** information warfare simulation games breakdown civil unrest rebellion

Source, Vol, No. UPI

Organizers from the Institute for Security and Intelligence's Center for Technology and Terrorism, with support from the Jane's company that publishes military magazines and books, brought together US government staff and industry executives in a war-game simulation that resulted in frighteningly believable attack scenarios. Instead of the usual dumb attacks directly eliminating their targets, these cyberwarriors concentrated on causing disruption with false information and denial of service. According to Pamela Hess writing for UPI, "The terrorists, determined to bring down the money-grubbing IRS, devised a diabolical plan with alarming speed. They would hack into the IRS audit system and send out millions of audit notices to American citizens, at the same time sending out "tax due" notices and jamming all the telephone, fax and e-mail lines into and out of the organization to give already irate citizens only busy signals. Just for fun, they tapped into immigration control and State Department systems to issue visas to known terrorists to come to the United States. They created fake documents to make it appear that the organization was investigating the personal lives of members of Congress, then leaked these to the media, along with fake compromising photographs."

Date 1999-11-20 **Keyword** information warfare study overview

Source, Vol, No. The Times (London)

Michael Evans, writing in The Times of London on November 20th, reported on the growing awareness of cyberwar as a real threat. Citing a number of military and law-enforcement authorities, he made a strong case for the likelihood of information warfare as a threat to developed nations.

Date 1999-11-23 **Keyword** Internet e-mail interception confidentiality industrial espionage

Source, Vol, No. UPI, San Jose Mercury News

In a settlement of one of the few documented cases of industrial espionage involving intercepted e-mail, the Alibris company paid a $250K fine for the firm it acquired in 1998. That company, Interloc, admitted intercepting and copying 4,000 e-mail messages sent to Amazon.com through its own ISP, Valinet. Prosecutors said that the e-mail was intercepted to gain a competitive advantage against Amazon in Interloc's own book business. The managers of Interloc steadfastly denied any wrongful intention but failed to explain why they copied the e-mail.

Date 1999-11-24 **Keyword** criminal hacker espionage political party bank accounts

Source, Vol, No. Reuters

The British Conservative Party complained that someone hacked into its bank accounts in an investigation (or smear) campaign around foreign donations. The Times of London denied that any of its journalists had done any such thing.

Date 1999-11-30 **Keyword** principles policy infrastructure protection infowar information warfare government industry assoc

Source, Vol, No. ITAA press release <http://www.itaa.org/infosec>

The Information Technology Association of America (ITAA) issued a Statement of Principles on 30 Nov 1999. ITAA's InfoSec Statement of Principles acknowledged the importance of protecting the national information infrastructure and highlighted private industry's primary authority for protecting it. The statement urged the lowest possible government regulation of critical infrastructure protection. The principles included a call for distinctions among cyber-mischief, cybercrime and cyberwar so that appropriate law enforcement agencies could take charge of specific cases with minimal jurisdictional confusion and with assurance of a clear legal basis for prosecution.

Date 1999-11-30 **Keyword** information warfare espionage hacking penetration government policy secret

Source, Vol, No. AUSTRALIAN; Newsbytes

In 1996, the Attorney General of Australia blocked distribution of a special report on information warfare techniques for the Australian Security Intelligence Organisation (ASIO). A censored version was grudgingly released under the Freedom of Information Act after demands from Electronic Frontiers Australia. However, in January, a student discovered complete copies of the restricted report in several public libraries. The report recommended measures that were later incorporated into legislation that authorized ASIO to use techniques typically associated with criminal hacking such as unauthorized penetration of systems, data modification, installation of Trojans and back doors, and computer surveillance.

Category 17 Penetration, phreaking (entering systems, stealing telephone service)

Date 1999-01-04 **Keyword** criminal hackers hacktivism sabotage information warfare

Source, Vol, No. Los Angeles Times

Maggie Farley, a Staff Writer for the Los Angeles Times, provided an in-depth review of "hacktivist" attacks on Chinese Internet sites. Groups such as Bronc Buster, Cult of the Dead Cow and the Hong Kong Blondes [a gang later found to have been a hoax] have been penetrating Chinese systems, vandalizing government or pro-government Web sites, installing back-door programs for later access and control, and sending out millions of news reports to Chinese recipients -- including even head of Shanghai's Internet security division -- from randomized e-mail source addresses (to escape identification and prosecution).

Date 1999-01-06 **Keyword** criminal hacker teenager social engineering administrator e-mail forged headers police arrest conf

Source, Vol, No. Straits Times (Singapore)

Goh Teck Hwee, 17, was arrested for posing as an official from the Singapore ISP SingNet. The top student in his class, he was impressed by the movie "Hackers"and began reading about hacking on the Internet. After learning how to alter the headers on his e-mail to pretend that he was "Dade Murphy" (a character in the movie) and told 20 SingNet users that their accounts were "corrupted." He demanded their user IDs, passwords, and billing information — and four gullible unfortunates complied. He stole ISP service at their expense for several months. He was arrested four days after one of the victims realized what was happening and reported the crime to police. Goh pled guilty to impersonation at his hearing and faced three other charges.

Date 1999-01-06 **Keyword** computer crime police enforcement prosecution punishment

Source, Vol, No. Xinhua News Agency (translated by OTC)

According to the official Chinese government news agency, 1998 was a banner year for the fight against computer crime in China. After several years of 30% annual growth, there were almost one hundred cases of computer crime cases were uncovered -- only a small portion of the total, according to the Public Security Ministry. One computer journal estimated that 95% of all Chinese network management centers exposed to the Internet had been attacked, whether by Chinese hackers or by foreigners. According to the Xinhua report, "In one study, Jinhua'an Information Technology Co. recently conducted tests of dozens of security agencies in Shanghai and Shenzhen, and found almost all of their network security systems were undefended. With a lap top computer hooked up to a telephone line, testers easily logged in their networks and reached restricted information in a minute."

Date 1999-01-06 **Keyword** criminal hackers Trojans password stealing BackOrifice Netbus theft services police warnings

Source, Vol, No. Herald Sun (Australia)

Police in Australia warned of a rash of penetrations of ISP users' computers using Trojans such a BackOrifice and Netbus. The victims reported huge bills after criminals stole their user IDs and passwords and racked up hours of connect time in their names. The trojans were discovered in all kinds of executables, including electronic greeting cards, games, and stolen software.

Date 1999-01-06 **Keyword** criminal hacker hospital pirated software intellectual property penetration vandalism

Source, Vol, No. Magyar Hirlap

Police in Pecs (southern Hungary) arrested a 22-year-old student in January 1999 who allegedly penetrated the databases of several hospitals and disabled their servers. He was also found in possession of illegally-copied software and may have been distributing copies. Police said this was the biggest computer hacking crime committed so far in Hungary. The student also possessed a CD from the Matav telecommunications company containing ownership of unlisted (ex-directory) telephone numbers. The student admitted breaking into the databases but did not admit disabling the hospital servers.

Date 1999-01-08 **Keyword** criminal hacker teenager child China Web penetration immunity

Source, Vol, No. Xinhua (PRC News Agency) via OTC

A 13-year-old middle-school student in the Inner Mongolia Autonomous Region of the People's Republic of China (PRC) managed to penetrate the Guangzhou province official Web site in southern China, where he posted a Web page entitled "Hacker." He then apparently obtained root on a multi-media telecommunication network for the Mongolian capital of Hohhot. Later he threatened to vandalize the main page of the "169"network, a major Mongolian ISP. The child was ruled immune to prosecution because of his age; the police ordered his parents to keep a closer watch on him. [Considering that some criminal hackers have been executed in China, one imagines this advice would be heeded.]

Date 1999-01-11 **Keyword** police criminal hackers phreaks theft telephone service PBX PABX private branch exchange

Source, Vol, No. Newsbytes

British police began a campaign in January 1999 to crack down on theft of telephone services through subverted private branch exchanges (PBXs). Criminals, including organized crime, were reported to use direct inward services access (DISA) to place long-distance calls at the victims' expense. Since many firms also provide toll-free access to their PBXs, they end up paying for the entire theft. [MK Comment: DO NOT LEAVE DISA ENABLED! Anything you can for legitimate employees using DISA you can also do using telephone cards — and be sure that those cards do NOT show the PIN for the account number.]

Date 1999-01-21 **Keyword** criminal hacker penetration home computer police

Source, Vol, No. AP

A 19-year-old Danish criminal hacker picked a home computer at random and began attacking it. Unfortunately, the computer belonged to Detective Arne Gammelgaard, head of the Copenhagen police's special computer crime unit. Gammelgaard's personal firewall informed him of the hack and he tracked down the malefactor immediately. The student admitted guilt and was convicted for "unauthorized access to another person's documents or programs." He faced up to six months in jail.

Date 1999-01-26 **Keyword** criminal hackers Web vandalism

Source, Vol, No. Defcon Hacker List

A tizzy in a teapot broke out when the HFG (Hackers for Girlies) vandalized criminal-hacker sympathizer Carolyn Meinel's Web site. The HTML source code included a great deal of abusive text attacking computer security celebrities such as Winn Schwartau and Fred Villella.

Date 1999-02-15 **Keyword** criminal hackers challenge contest penetration testing perimeter Japan

Source, Vol, No. JIJI PRESS NEWSWIRE

International Network Security Inc. of Tokyo appealed to criminal hackers to break into their company's computer systems as an employment test. The new company offered penetration testing, although how it would guarantee its customers' safety given the nature of its proposed employment strategy was not spelled out. The president of the company, Sato Hideaki, is said to be a close friend of Mark Abene, the criminal hacker who spent nearly a year in jail for his part in the depredations of the Legion of Doom and who was responsible in 1997 for accidentally broadcasting a command on the Internet that resulted in his receiving thousands of password files from computers around the world.

Date 1999-03-01 **Keyword** criminal hacker punishment sentence court fine damages

Source, Vol, No. RISKS 20 23

Peter G. Neumann coined a new term: "PGNed" which he modestly defined as "summarized in an abstract." In my opinion it means "brilliantly summarized." Here is a PGNed item about a criminal hacker from Rhode Island: "Sean Trifero was sentenced to one year in prison by a U.S. District Judge for intentionally damaging computer systems (Harvard, Amherst, a Florida ISP, and Alliant Technologies, including planting sniffers and denial-of-service attacks) and unauthorizedly accessing others (Arctic Slope Regional Corp. and Barrows Cable, Alaska), three years subsequent probation, 150 hours of community service, and $31,650 restitution."

Date 1999-04-22 **Keyword** impersonation social engineering ISP credit card password

Source, Vol, No. RISKS

I recently received an obviously fraudulent e-mail request claiming to be from CompuServe administration and demanding that I submit my user-ID, _password_, and full credit-card information. After I forwarded it to CompuServe support I received a response with the following key text:

> There are currently numerous email messages circulating on
> the service claiming to be official CompuServe notices of account
> and/or billing problems being sent to members which contain
> a form that is supposed to be filled out and returned by email
> or a termination of the account will occur. It is an attempt
> to steal your credit card and CompuServe account information!
>
> DO NOT respond to this or any similar email!
>
> Instead forward a copy of the complete message by email
> to the CompuServe Internet address actionteam@compuserve.com.

RISKS readers may want to remind naive users of any ISP be warned never to respond to requests to reveal their passwords to anyone at an ISP or indeed, on any network. Even in the rare cases where it would be useful to log into a specific account for problem resolution, any authorized personnel who need access to an account will have the capabilities required to change its password themselves. They do not need to know the user's original password.

Date 1999-04-27 **Keyword** hacker confederate guilty plea law court justice

Source, Vol, No. LA Times

In April, Lewis DePayne pleaded guilty to conspiracy to defraud the Nokia Corporation in his attempt to help Kevin Mitnick steal software. He admitted having used social engineering techniques against Nokia, impersonating an employee to gain access to systems. Prosecutors dropped 13 other criminal charges against DePayne and recommended leniency in sentencing (six months of home detention or community confinement, five years of probation, 225 hours of community service and a fine of $2,000 to $5,000).

Date 1999-05-12 **Keyword** criminal hacker hacktivists Web defacement alert

Source, Vol, No. ANSIR / NIPC Advisory 99-008

The National Infrastructure Protection Center (NIPC) issued an Awareness of National Security Issues and Response (ANSIR) alert in May 1999 warning that a hactivist group called F0RPAXE defaced several US military and government Web sites. The group claimed to be a Portuguese organization opposing the Portuguese government.

Date 1999-05-13 **Keyword** hacking contest firewalls

Source, Vol, No. Reuters

Reed Exhibition Companies of Singapore launched a one-week hacking contest in May 1999. Successful hackers who could vandalize three Web sites protected by various firewalls would win prizes of U$10,000 and S$10,000 (U$1=S$1.70). Critics disapproved of rewarding what would otherwise be criminal activity and complained that such "hack-off"contests reveal little of value about the security systems under attack.

Date 1999-05-19 **Keyword** insider sabotage forgery fraud witness-tampering lawsuit dismissal investigation

Source, Vol, No. AP

In April 1998, Christian Curry was fired by Morgan Stanley Dean Witter, ostensibly for abusing his expense account. Mr Curry claimed at the time that he was fired because he is black and because his employers thought he was a homosexual (he isn't). While waiting for a response to his claim for wrongful dismissal, Curry talked to an old college buddy of his, C. Joseph Luethke, about planting forged e-mail in the company system to demonstrate homophobia and racism. Luethke reported the conversation to the company and sent Curry to a private detective who pretended to be a criminal hacker. Curry paid the "hacker" $200 for insertion of the forged e-mail and was then arrested on charges of forgery, coercion and tampering with physical evidence. However, the lurid story wasn't over yet: it turned out that Morgan Stanley paid Luethke, the "friend," $10,000. In May 1999, all charges against Mr Curry were dropped and he and his lawyers were contemplating a lawsuit against Morgan Stanley, accusing the firm of libel, conspiracy and violating Curry's human rights.

Date 1999-05-28 **Keyword** criminal hackers attack government Web sites down unavailable vandalism defaced

Source, Vol, No. AP, New York Times, Newsbytes

Criminal hackers attacked several US government Web sites, including those of the US Senate and the FBI, apparently in retaliation for FBI actions against Eric Burns ("Zyklon"), who was indicted in May on three counts of illegal computer intrusions. The FBI shut down its Web site to increase security. The Senate Web site included the following hacker-lingo: "The FBI may be all over the other groupz, like those gH and tK queerz, cl00bagz gal0re. M0D make th0se m0ronz l00k like a gr0up of special-ed st00dentz! FBI vs. M0D in '99, BR1NG IT 0N FUQRZ! (BTW NIPC IZ ALS0 0WNED)... S0METIMEZ U G0TTA G0 WITH A NAME U CAN TRUST. 4 S0ME, REGULAT10N IZ JUST A WAY 0F L1FE. 0wned (0wn'3d) : the art of showing how stupid a sysadmin can be, see sekurity." Global Hell (gH) was thought to be the criminal-hacker gang that attacked the FBI. The vandals signed their masterpiece, "Mast3rz 0f D0wnl0ading."

Date 1999-05-28 **Keyword** criminal hacker subculture gang group Russia

Source, Vol, No. Unknown source, Moscow Times

A Russian criminal hacker gang calling itself Chaos Hackers Crew has been wiping out home pages around the world. They steal access codes for ISPs and appropriate services for their nefarious hobby; their criminality made AOL and CompuServe decide to abandon Russia altogether.

Date 1999-05-31 **Keyword** criminal hacker gang syndicate organized crime Asia police arrests

Source, Vol, No. Newsbytes

In one of the first successful crackdowns on organized computer-crime syndicates, Hong Kong police arrested ten men accused of stealing and reselling illegal access to ISPs. They allegedly stole account information from at least 200 victims and then sold the accounts to thieves who wanted unlimited access to the Net. The gang also sold CDs with pirated music.

Date 1999-06-01 **Keyword** criminal hackers Web sites extortion defaced attacks vandalism political government

Source, Vol, No. AP

The Portuguese criminal hacker group F0RPAXE defaced Web sites of the US Department of the Interior and of the Federal Supercomputer Laboratory in Idaho Falls, ID. The vandals left a note boasting that unless the FBI stopped investigating criminal-hacker gangs in the US, they would destroy government systems.

Date 1999-06-02 **Keyword** criminal hacker investigation Web vandalism defacement seizure

Source, Vol, No. New York Times

The FBI raided several suspected criminal hackers in late May in connection with the wave of attacks on US government Web sites. Paul Maidman, 18, of Waldwick, NJ denied that he was involved in the attacks. However, he admitted, "I got into other servers. I'd look around, read some e-mail, and that would be it." The FBI seized his computer, some diskettes and CD-ROMs. According to reports posted on the Internet, the FBI obtained warrants to require several ISPs to release information about dozens of criminal hacker gangs, pseudonyms and hacking tools.

Date 1999-06-03 **Keyword** criminal hacker probes attacks intrusion detection

Source, Vol, No. Computing (UK)

Howard Schmidt, Director of Information Security at Microsoft, told the Infowar 99 conference in London that the giant software company has detected up to 22,000 probes an hour in attacks on one of its data centers. He said that most of the attacks were from "ankle-biters" (children) trying to raise their status in the criminal hacker underground. He made a special point of warning managers to protect their PBXs against penetration by updating passwords regularly. Microsoft uses the Info.Safe method of having constant challenges to their own networks by Red Teams; employees who detect the attacks win special tee-shirts.

Date 1999-06-11 **Keyword** criminal hacker hactivist attacks Web vandalism

Source, Vol, No. UPI

F0RPAXE, the supposedly Portuguese criminal hacker gang, continued its attacks on governments and universities in the US. They apparently penetrated the Web site of the Illinois State Comptroller's Office, where they vandalized the home page and ridiculed the FBI.

Date 1999-06-12 **Keyword** Web attack criminal hackers government

Source, Vol, No. AP

A new criminal hacker group calling itself Varna Hacking Group (Varna is the name of a Bulgarian province) successfully attacked the Web site of the US Senate — the second hack in two weeks. The criminals hijacked visitors to the site, redirecting them to a Web site on a Florida hosting service where a modified version of the official site was located. The copy of the Web page included ridicule of the FBI; an obscene, anonymous message on the real Senate Web site claimed that the attack was motivated by the desire to stop FBI investigations of criminal hacker groups.

Date 1999-06-17 **Keyword** criminal hacker ISP account abuse theft services stealing password

Source, Vol, No. New Zealand Herald

A 24-year-old Auckland NZ man was arrested and charged with stealing more than $600 of ISP services using a victim's account. The theft was discovered when the victim switched from an unlimited-usage account to a less expensive 10-hour a month account. The thief was identified with the help of ISP log files.

Date 1999-06-26 **Keyword** criminal hacker penetration theft embezzlement transfer bank Russia sentence imprisonment priso

Source, Vol, No. RIA (Russian news agency) monitored by BBC

In June, two young Russian hackers were imprisoned for 6.5 and 7 years for having stolen a large amount of money (the news reports are unclear on the exact amount) using a computer program to embezzle the funds from the Berezniki branch of Sberbank in 1997. Igor Chupin and Igor Chernyy [sic] transferred the funds into their own bank account. They took out cash from banking machines in Perm, Moscow and St Petersburg over the next three days. That money was never recovered. The court sentenced these criminals to 7 and 6.5 years in prison, respectively. In addition, the young men are supposed to pay restitution and fines amounting to R2,782,000 (U$28,869), a sum so vast by Russian standards that the Moscow news report ended with the comment, "Judging by everything, they will have to pay the bank as long as they live." [Mind you, in the Russian prison system, that may not be very long.]

Date 1999-08-10 **Keyword** criminal hacker court case law judgement punishment prison fines restitution parent father morali

Source, Vol, No. SJ Mercury News, Los Angeles Times, Guardian (London), Reuters

Criminal-hacker icon Kevin Mitnick finally negotiated an agreement with prosecutors in California. Mitnick, imprisoned for the last four years much to the disgust of criminal hackers and their sympathizers everywhere, agreed to an additional year of imprisonment and a three-year period thereafter during which he would not use computers. At his sentencing hearing in August 1999, he was also ordered to pay a token $4,125 in restitution and to turn over all profits from any books he may write or interviews for which he may be paid. Mr Mitnick's father said he was proud of his son, whom he said had a lot of talent and was unfairly targeted by prosecutors. "A lot of people made their fortunes off his name," said Alan Mitnick. "He was made to be a poster boy. They wanted to scare other hackers in the future. They also want to control the information superhighway."

Date 1999-08-11 **Keyword** criminal hacker probes Trojans back door

Source, Vol, No. Bangkok Post (Thailand)

A question-and-answer column in the Bangkok Post, Thailand in August 1999 showed how widespread criminal hacking has become in this Internet-assisted age. Howie Mirkin wrote, "In the past two weeks I have experienced about three to four "back orifice" hacking attempts per day. I have a small program called anti-BO, which detects such attempts. I have been notifying the appropriate ISPs after doing a WhoIs ISP Lookup and a trace route to help them determine the user.
The anti-BO program gives the time and host id. I have had a couple of ISPs come back and tell me that they throw hackers off their connection, but we know that nothing will stop them if they want to hack. . . . It is a real pain to keep getting these hits and have to stop working and gather data to report them. Are there any laws about this? What I really wonder is how many people are getting hacked without knowing it because they have no detection program."

Craig Emmott, Director of Support Services of Internet Thailand, responded, "Unfortunately, scanning for backdoor programs such as Back Orifice is very common these days. If ISPs are informed of the time and origin-IP of the scanning they can contact the owner of the account being used at the time. However, this will often turn out to be a hacked account or the owner will deny all knowledge of the incident. Until the TOT and TA provide caller-ID on modem access lines, there is little ISPs can do other than advise these account owners to change their password." He added, "Generally, these would-be hackers don't target any specific individual. Instead, they scan whole blocks of dialup lines belonging to target networks. The main objective is to steal passwords and use them to get some free Internet access at other users' expense." Finally, he commented, "There are now over 100 backdoor/Trojan programs available on the Internet, but Back Orifice and NetBus are still the big favourites in Thailand. The most practical defence against them is to only run software from trusted sources and to use one of the major anti-virus products, all of which can detect the most widely used Trojans."

Date 1999-08-18 **Keyword** criminal hacker hoax lie manipulation press gullible evidence investigation fraud spoof media

Source, Vol, No. IT Daily (AsiaTech)

Investigation of the supposed depredations of the "Hong Kong Blondes" strongly suggested that the criminal hacker gang supposedly led by "Blondie Wong" was a hoax by the Cult of the Dead Cow.

Date 1999-08-31 **Keyword** back door e-mail script Web confidentiality bug

Source, Vol, No. PA, Wired <http://www.wired.com/news/news/business/story/21490.html>

In August, two serious security holes were demonstrated on the HotMail servers run by Microsoft and claimed to be the biggest free Web-mail system in the world, with millions of subscribers affected. The problems were as follows:
(1) An error in the code for entering data into a form allowed a user login without any password at all;
(2) An undocumented back door allowed anyone to log in to any HotMail account using the canonical password "eh."
These problems meant that all unencrypted HotMail e-mail was readable to anyone who used the exploits and that such people could also impersonate their victims through e-mail. The holes caused Microsoft to shut down access to HotMail for a day while the vulnerabilities were removed.

The perpetrators, calling themselves "Darkwing" and "Hackers Unite," took responsibility for the hack. The criminal hacker spokesperson was Swedish computer expert Lasse Ljung, who said, "Hackers Unite hacked Hotmail because they wanted to show the world how bad the security is on Microsoft. . . . It is a big company on the net, so it wasn't to destroy it for others, it was to show the people how bad the security is."

Date 1999-09-02 **Keyword** criminal hacker denial of service punishment jail prison China vandalism

Source, Vol, No. Xinhua

Lu Xuewen, 24-year-old high school graduate in Guanzhou (formerly known as Canton) in the PRC, penetrated the mainframe of government-owned ISP Chinanet and also a BBS server using stolen account numbers in January and February 1998. He created additional accounts for himself on the system and crashed the system for 15 hours. He was jailed for 18 months under the Criminal Law of 1997 that updated statutes to make unauthorized access to computer systems a crime.

Date 1999-09-10 **Keyword** Y2K criminal hacker quality assurance tests electricity power

Source, Vol, No. Wall Street Journal

According to a report in the Wall Street Journal, the successful Y2K-compliance tests carried out in early September by the North American Electric Reliability Council (NERC) with the involvement of over 500 utilities, electric cooperatives, power pools and power plants were marred by a criminal-hacker penetration of the Bonneville Power Administration center, where the Secretary of the Department of Energy, Bill Richardson, was observing the tests.

Date 1999-09-17 **Keyword** criminal hacker gang disruption penetration

Source, Vol, No. New Straits Times (Malaysia)

According to a spokesperson for the Malaysian ISP, Jaring, a group of users based in a Malaysian university were responsible for breaking into at least 18 organizations and controlling more than 38 servers. The criminal hackers were among a large worldwide group causing harm to Undernet, one of the world's larges IRC channels. The Malaysian CERT put up recommendations for improving security on its Web site at <http://www.mycert.mimos.my>.

Date 1999-09-20 **Keyword** magazine hacking contest quality assurance encourage criminal hackers legitimize hacking

Source, Vol, No. PR

PC Week Labs staged an unfortunate quality assurance contest pitting criminal hackers and others against a servers running LINUX Windows NT. The magazine challenged anyone to break into the Web site, as if such a test could be a reasonable demonstration of the security characteristics of the two operating systems. Those who successfully "mark up the home page and steal user information from the classified-ads engine" would be rewarded with computer equipment and gift certificates for about $1,000.

Date 1999-09-24 **Keyword** criminal hackers hactivisits political Web site defacement vandalism propaganda

Source, Vol, No. Detik (Jakarta) via BBC Monitoring Service

Indonesian Web sites were hacked by pro-Timorese hactivists starting in September 1999. The Antara Web site was defaced, with the following message left in place of the anodyne commercial text: "Indonesian Military Sponsors Mass Genocide 250,000 DEAD since 1975. How can you condone this? Your leaders have no respect for human rights. Will they have respect for yours? Your army has supported armed and trained anti-independence DEATH SQUADS in East Timor. Indonesia itself gained independence. Why has Indonesia then destroyed East Timor's dream of freedom? It is better to live one day in freedom and die than live a lifetime in the yoke of an oppressor."

Date 1999-09-29 **Keyword** criminal hacker bank financial transactions penetration credit card confidentiality

Source, Vol, No. Scotsman

Frans De Vaere admitted breaking into the Web site of a Belgian bank in mid-August. He stole logon IDs and passwords and successfully accessed the account balances of many customers; luckily he was unable to effect any transactions. The bank, identified as "Generale de Banque" in a report by Alex Blair in _The Scotsman_ newspaper, refused to take legal action against the criminal hacker. However, the Skynet ISP run by the state telecom company, Belgacom, was not so accommodating. The criminal hacker broke into more than 1,000 Web sites on Skynet and stole the credit-card numbers of about 20 clients. Police began an investigation, but unfortunately Belgium has no specific law addressing computer crime and so the intruder is still unpunished.

Date 1999-10-14 **Keyword** criminal hacker threats vulnerability critical infrastructure electric power utilities damage

Source, Vol, No. Dow Jones

"Mudge" (Peiter Zatko), a member of the L0pht, claimed in mid-October 1999 that he would release a report on security vulnerabilities at about 30 electric power utilities in the US whose grids he claimed he could shut down easily. In a welcome change from other cases involving unauthorized probes of networks, Zatko said that the L0pht would give the utilities a chance to see the report and fix the vulnerabilities before they were posted in public.

Date 1999-10-14 **Keyword** criminal hacker ISP theft of service vulnerability

Source, Vol, No. SMH

In an odd twist, the Australian ISP FreeOnline treated a criminal hacker respectfully after he claimed in the Oz version of _2600_ magazine that it was possible to use the ISP without registering for a userID and password. Members of the criminal hacker magazine's club affirmed that the exploit was in fact being used successfully despite the denials of the ISP's technical staff that there was a vulnerability. The company's CEO, Sydney Low, said, "If Pho can show us that there is a flaw we'll pay him $100 an hour, because we're happy to support behaviour that increases the smarts of the industry. While we don't want to stifle this kind of activity, we don't think he should have posted the hack to a Web site without confirming its legitimacy with us first." [This kind of statement gives succour to the enemy and feeds the propaganda engine of the criminal underground. There is no place for acceptance of people who break into systems, steal services, and then boast about their exploits in detail so that other criminals — and children — can imitate their behavior.]

Date 1999-10-18 **Keyword** hacking contest quality assurance test trial exposure

Source, Vol, No. Reuters

The Shanghai Waigaoqiao Free Trade Zone Network Development Co. offered anyone who could break into their Web site 5,000 Yuan (U$600) in mid-October 1999 during a one-week trial.

Date 1999-10-20 **Keyword** criminal hacker punishment prison appeal sentence judgement government

Source, Vol, No. Straits Times (Singapore)

Muhammad Nuzaihan Kamal Luddin, a 17-year-old high school student in Singapore, hacked into Swiftech Automation and Singapore Cable Vision and was sentenced to 2-1/2 years on probation by a district dourt in June 1999. However, the government appealed the sentence and won a stricter penalty for the young man's criminal activities: four months in jail. The decision sparked a vigorous debate about the suitability of imprisonment as a punishment for criminal hacking by young people.

Date 1999-10-21 **Keyword** criminal hackers Israel politics police law enforcement prosecution court phreaking theft of servic

Source, Vol, No. Wall Street Journal

In October 1999, the Israeli government finally began the trial of two blind Israeli Arab brothers, Munther and Muzhir Badir. The two were suspected of a series of major attacks on telephone systems for call-sell operations, fraudulently selling other people's land, and credit-card fraud. The indictment included 47 different counts of criminal activity. The flamboyant brothers became celebrities in Israel, with regular interviews in the media. The bitter intercommunal relations of Jews and Arabs in Israel complicated the case, with many opponents of the Israeli government claiming that the brothers were abused in the notoriously rough Israeli jails. In one interesting wrinkle, Munther Badir claimed that he worked for the Labor Party in 1998; he said he had sabotaged the party's system and then repaired it, blaming the crash on the Prime Minister's political opponents. However, Labor Party officials denied any record of Badir's working for them.

Date 1999-11-03 **Keyword** criminal hacker penetration ISP passwords

Source, Vol, No. AAP, Courier Mail (Brisbane)

Someone broke into the Australian Optus Internet ISP on 1999-11-03. The ISP contacted its 100,000 customers and told them to change their passwords for Internet logon. Police were investigating.

Date 1999-11-11 **Keyword** criminal hacker prison penetration vandalism Web passwords theft

Source, Vol, No. AP

In Singapore, Pang Soon Chen, 19, and David Kok, 22, were sentenced to 15 and 8 months in prison respectively for breaking into 54 Internet users' computers and stealing their passwords. The two also posted the passwords to a Web site in the US.

Date 1999-11-17 **Keyword** information warfare attack criminal hacker contest challenge firewalls

Source, Vol, No. Xinhua (Beijing)

In October, a Shanghai company issued a challenge to hackers to test its Web site security. The site was attacked 76,250 times in the first two weeks of the challenge, with peak rates of 1,253 attacks per second. No known penetration occurred.

Date 1999-11-23 **Keyword** criminal hacker punishment conviction trial Web vandalism

Source, Vol, No. AP

Eric Burns, 19, pleaded guilty in September was convicted in November 1999 of criminal hacking and admitted that he had vandalized many other Web sites, including the White House site, in May. Despite his sentence of 15 months in prison and three years of supervised probation along with restitution of $36,240, the lad said, "I didn't really think it was too much of a big deal." Cost of recovering the government sites was estimated at $40,000. Burns, who called himself "Zyklon" after the gas used by Nazis to murder Jews in death camps, said he thought his penalties were too severe and vowed not to identify his two confederates. "I don't really agree with the kind of sentencing range there is for the crime."

Date 1999-12-06 **Keyword** inside job criminal hackers hactivists political penetration information warfare INFOWAR

Source, Vol, No. Daily Telegraph (UK)

Criminal hackers (or possibly insiders) penetrated the computer systems of the Palestine Liberation Organization in December 1999. The unknown assailants published secret information about Chairman Yasser Arafat's billions of dollars of savings in secret Swiss numbered bank accounts and extensive land holdings in various European cities. Daily Telegraph writer Tom Gross reported, "The computer security breach is believed on the West Bank to have been carried out by PLO officials disgruntled with Mr Arafat's leadership."

Date 1999-12-08 **Keyword** criminal hacker gang telephone services abuse phreaking credit-card theft fraud plea court trial

Source, Vol, No. UPI

In 1995, FBI agents raided a ranch in a rich neighborhood north of San Diego and confiscated Jonathan Bosanac's computer. In December 1999, the now-27- year-old criminal hacker pleaded guilty to what police were calling the largest computer hacking scheme in US history. The gang led by Bosanac (aka "The Gatsby") broke into computers at AT&T, MCI and Sprint (among others) and stole thousands of calling card numbers which they sold to other criminals at $2 each. The cards were then used to make thousands of illegal long-distance phone calls. The gang also forwarded an FBI telephone number to a phone-sex line, racking up $200,000 in embarrassing phone bills. At one point, they harassed a victim by automatically sending his phone number to thousands of pagers. in September, the courts sentenced two other criminals in what the FBI called the Phonemasters to jail terms: Corey "Tabbas" Lindsley got 41 months in prison and Calvin "Zibby" Cantrell received a 24 month term. Seven other defendants in the case had already pleaded guilty in federal court and were awaiting sentencing. Bosanac was to be sentenced on 2000-03-02.

Category 18 Theft of equipment (laptops, ATMs, computers, cables, network components)

Date 1999-01-01 **Keyword** theft computer components organized crime

Source, Vol, No. UPI

On 31 December 1998, three members of Asian organized crime syndicates were convicted in Los Angeles of the largest theft of computer components in history. According to the UPI report, "The robbers escaped with $2 million worth of hard drives in a March 25, 1995, heist at Comtrade Electronics in City of Industry, CA and nearly $400,000 in computer components from Multi-Industry Technology in Cerritos, CA on May 3. The third crime . . . took place at Centon Electronics in Irvine, CA where approximately $10 million worth of computer chips and motherboards were stolen by the armed bandits."

Date 1999-01-05 **Keyword** denial of service theft breakin violence

Source, Vol, No. RISKS 20 15

Three armed robbers broke into a Boston-area Sprint telephone office, assaulted workers with stun guns, tied them up, and stole telephone switches. The robbery interrupted service for 75K users for 7 hours.

Date 1999-04-08 **Keyword** theft laptop computer components equipment organized crime

Source, Vol, No. GUARDIAN

In Britain, the _Guardian_ newspaper reported on the professionalization of computer theft — the physical abduction of computers, that is. A Home Office study, called "Pulling the Plug on Computer Theft," reported the following key findings:
* many of the "second-hand" computers for sale through classified ads are stolen;
* total value of stolen computers approached £320M per year in 1996;
* 96% of a sample of 1,048 stolen items recovered by police were computers or computer-related hardware;
* professional gangs find it ridiculously easy to study unsecured targets such as universities and hospitals where there are few barriers to free access;
* any organization that has been burgled is more likely to be attacked again;
* most thefts were burglaries carried out after hours by breaking through minimal barriers, but a few were armed robberies in broad daylight.

Category 19 Counterfeits, forgery (including software piracy but not impersonation)

Date 1999-02-15 **Keyword** software piracy theft copyright infringement copy CD-ROM

Source, Vol, No. San Jose Mercury News

In Beijing, a court ordered two software pirates to compensate Microsoft for stealing their software and making illegal copies. This was the first case in which the Chinese justice system condemned miscreants for violations of intellectual property rights.

Date 1999-02-16 **Keyword** credit card counterfeit fraud organized crime Asian Triads

Source, Vol, No. PA News

According to the British National Criminal Intelligence Service, the explosion in credit-card counterfeiting and other credit fraud is largely due to increased activity by Asian Triads. Losses grew by 500% between 1991 and 1998, with total theft estimated at £25M in the UK in 1998.

Date 1999-02-19 **Keyword** counterfeit pirated copies intellectual property copyright violation organized crime CD software

Source, Vol, No. AP

According to investigative reporter Nicolas B. Tatro writing for AP, Israel is a hotbed of counterfeiting and supplies large numbers of pirated CDs with stolen software distributed with the help of Palestinian criminal organizations in the West Bank. Uncollected royalties may amount to $170M a year to US copyright holders. Other counterfeit products include millions of audio cassettes selling for a fraction of the legal cost. Some Israeli musicians are withholding new music, hoping to pressure their government into cracking down on the pirates. The Israeli government announced plans to increase the severity of sanctions against copyright infringement and created a new 10-member police team to attack the problem.

Date 1999-02-23 **Keyword** software piracy theft copyright infringement illegal copying

Source, Vol, No. UPI

According to a study by Microsoft Corp., software piracy in Virginia alone in 1997 caused the loss of nearly 5,000 jobs and more than $900 million in combined wages, tax revenues and retail sales.

Date 1999-03-25 **Keyword** lawsuit intellectual property music copyright infringement

Source, Vol, No. Financial Times

The Norwegian company FAST makes software that can download MP3 files. The International Federation of the Phonographic Industry (IFPI) lodged a complaint that resulted in criminal prosecution of FAST for facilitating the theft of illegally posted copyrighted music from the Web. The IFPI was also contemplating a complaint against Lycos, whose search engine catalogs these illegal snippets of intellectual property.

Date 1999-04-29 **Keyword** software theft copyright intellectual property piracy

Source, Vol, No. AP via OTC

Microsoft sued 15 Florida counterfeiters who sold copies of Windows 95 and Windows 98 without authorization. According to a study from International Planning & Research Corp., a market research company commissioned by Microsoft, software piracy cost Florida 7,186 jobs in 1997 and $490 million in lost wages, tax revenue and retail sales.

Date 1999-04-30 **Keyword** software piracy intellectual property theft misappropriation costs

Source, Vol, No. San Jose Mercury News

According to Bradford Smith of Microsoft, his company alone has lost more than $6B due to Chinese and other software piracy. Colleen Pouliot of Adobe estimated that 40% of all business applications are used without permission — a staggeringly damaging depression of the industry's production.

Date 1999-10-04 **Keyword** theft piracy counterfeit intellectual property contraband Internet Web upload download software

Source, Vol, No. Reuters

Jim Loney wrote a summary for Reuters news wire of the losses due to piracy of intellectual property and counterfeiting. Some key points:
* US Customs Commissioner Bonni Tischler predicted that copyright violations and counterfeiting was "going to dwarf every type of crime in the next millennium."
* U.S. companies have estimated they lose $200B a year to product piracy involving designer clothes, shoes, handbags, software, CDs and videos.
* World-wide, software piracy costs industry $11B a year.
* 38% of the 615M new software product installations were illegal copies.
* 97% of all the software in Vietnam was stolen.
* 90%+ of all software was stolen in Bulgaria, China, Indonesia, Lebanon, Oman, and Russia.
* 60% of the software being sold by auction on the Net is illegitimate.
* Criminals are setting up shop in jurisdictions with no cyberspace laws or lax law enforcement (such as Russia) and selling stolen property all over the world.
Loney concludes, "Customs officials say judicial systems lag behind exploding crime on the Internet. Cybercrime is difficult for juries to visualize, penalties are small and the risk of jail is minimal in comparison to crimes like armed robbery."

Date 1999-11-30 **Keyword** ATM automated teller machines fraud forgery confidentiality fake cards convictions

Source, Vol, No. DAILY TELEGRAPH

Two criminals in a British "hole-in-the-wall" gang were convicted of fraud and theft in Middlesex Crown Court at the end of November. The gang specialized in adding equipment to automatic banking machines to record card numbers and PINs. They would then manufacture forged cards and withdraw small amounts from each card, often thereby evading the notice of their victims; total thefts were estimated to be in the millions of pounds. According to British police, all the major banks had been victimized. The ringleaders of the scam remained at large.

Date 1999-12-01 **Keyword** ATM automated teller machines counterfeit cards fraud international

Source, Vol, No. MOSCOW TIMES

In October 1998, reports surfaced of organized data theft from banks in Moscow, where unsuspecting users of automated teller machines (ATMs) were the victims of a crime ring that used their stolen card information and PINs to create counterfeit cards that were then used for unauthorized withdrawals in several European cities. Both VISA and Europay accounts were charged; the companies have stated or implied that their Russian agency, Union Card of Moscow, was heavily involved in the fraud. The first arrests occurred in March 1999, when four Kazakh nationals were arrested in Munich with counterfeit cards at an ATM; they were convicted of organized credit card forgery and sentenced to up to 4 1/2 years in jail. Other arrests in the case were made throughout 1999 in Stockholm, Paris and London. The London arrest of Krister Elgsgem, a 32 year old Swedish man, occurred by chance in late November; an off-duty policeman was in line immediately behind the criminal as he fed about 50 obviously counterfeit (white, without logo) bank cards into an ATM. Russian police authorities have issued no statements about their investigation.

Date 1999-12-08 **Keyword** credit card theft cookies Web browser embarrassment

Source, Vol, No. Network News

Eric Schmidt, CEO of Novell, was embarrassed when a criminal stole his credit-card information and bought more than 100 copies of Netware's chief competition, Windows NT. Schmidt guessed that the thief may have used (Trojan?) software that used cookies stored on his PC to obtain personal information.

Category 1A Sabotage (excluding Web sites)

Date 1999-04-14 **Keyword** sabotage virus criminal hacker penetration revenge employee

Source, Vol, No. HERALD SUN (Australia)

In Melbourne, Australia, a 33-year-old network administrator pleaded guilty to three charges of damaging property and 30 charges of computer trespass. Mr Ya Ge (Jacob) Xu admitted hacking into his former employer's systems at Integraph Public Safety to plant a virus and to "cause trouble" for revenge when he was refused acceptable payment for unpaid overtime. He was fined A$6,000 but was not sentenced to jail time.

Date 1999-04-29 **Keyword** sabotage disgruntled employee revenge Trojan logic bomb

Source, Vol, No. Herald Sun (Australia)

Karen Collier reported in the Herald Sun (Australia) about the growing incidence of sabotage for revenge by enraged employees or ex-employees. According to the author, "Hundreds of cases of angry staff wiping files, planting viruses, stealing trade secrets and spreading electronic rumors are already being reported each year in Australia."

Date 1999-09-29 **Keyword** criminal hacker vulnerability sabotage demonstration

Source, Vol, No. Scotsman

In early August 1999, a criminal hacker calling himself "Red Attack" (Frans de Vaere) threatened Belgian firms with electronic sabotage in a misguided attempt to draw attention to security vulnerabilities. A few weeks later, a different person claimed _he_ was the _real_ Red Attack and said that he would switch Belgian electrical power off for a couple of hours on September 29th as well as breaking into the Belgian Prime Minister's e-mail account. After earnest conversations with a company director of the Electrabel utility, the idiot agreed that maybe his demonstration wasn't such a great idea after all. In the event, the threats all evaporated. Was this yet another hoax perpetrated on gullible journalists and officials?

Date 1999-09-30 **Keyword** availability service disruption cable Internet traffic slow backhoe

Source, Vol, No. New York Times

An Ohio gas company worker accidentally cut a 40 Gbps east-west optic fiber cable at the end of September (an example of the notorious "backhoe attack"). Internet traffic was slowed as much as 50 times as terabits of data were rerouted through alternate connections. Repairs took about a day.

Date 1999-10-16 **Keyword** backhoe attack denial of service accident fiber optic cable cut

Source, Vol, No. RISKS 20 64

On 1999-10-16, a backhoe accident destroyed a major fiber-optic cable in Massachusetts. AT&T, MCI Worldcomm, and the Mass Turnpike Authority lost channels, resulting in major problems for people on the East coast of the US.

Date 1999-11-26 **Keyword** backhoe attack denial of service accident fiber optic cable cut

Source, Vol, No. RISKS 20 13

In Canada, a railway backhoe operator severed an AT&T Canada optic fiber cable on 1999-11-26, causing computer crashes, shutdown of phone lines and communications problems throughout southern Ontario. The Bank of Nova Scotia was without computer services and Internet services were slow because rerouted connections went through the US on the Thanksgiving holiday there.

Date 1999-12-13 **Keyword** information warfare sabotage hacktivists political anti-corporate

Source, Vol, No. Globe and Mail (Canada), < http://www.rtmark.com >

The battle between etoys (www.etoys.com) and etoy (www.etoy.com) brought to light a remarkable group of saboteurs calling themselves ®™mark (pronounced "artmark") who organized all kinds of shenanigans normally associated with criminal hacking (denial of service attacks on eToys.com servers in a "virtual sit-in") and information warfare (depressing the value of eToys.com stock using propaganda). See < http://www.rtmark.com >.

Category 1B Criminal hacker scene (conventions, meetings, testimony, biographies, publication

Date 1999-01-06 **Keyword** criminal hacker capture fugitive escaped parole violation

Source, Vol, No. AP

Convicted criminal hacker Justin Petersen was arrested on Dec 11, 1998 in Los Angeles after three months of parole violation. The generally-reviled criminal was known as Agent Steal for his tendency to steal information, defraud victims and betray his acquaintances to the police. He tampered with a radio contest by seizing control of its telephone lines and claimed to have led the FBI to equally notorious hacker icon Kevin Mitnick. He absconded from the halfway house in which he was to have served his remaining three years of incarceration (after 3.5 years in penitentiary). He posted arrogant messages on the Internet sneering at the FBI -- not a measure calculated to let the federal police lose interest in him.

Date 1999-01-08 **Keyword** criminal hackers statements hacktivism ethic propaganda

Source, Vol, No. National Post (Canada)

After the Legion of Underground (LoU) announced on the 1st of January 1999 that they would attack and disable the computer systems of the People's Republic of China and of Iraq, a coalition of criminal hacker organizations announced opposition to the move. Eric Corley (using his pseudonum "Emmanuel Goldstein"), editor of _2600: The Hacker Quarterly_, signed the statement from Cult of the Dead Cow, Chaos Computer Club, !Hispahack, LOpht, Phrack, Pulhas, and Toxyn. "This kind of threat, even if made idly, can only serve to further alienate hackers from mainstream society and help to spread the misperceptions we're constantly battling. And what happens when someone in another country decides that the United States needs to be punished for its human rights record? This is one door that will be very hard to close if we allow it to be opened," said Corley in the statement. "We strongly oppose any attempt to use the power of hacking to threaten or destroy the information infrastructure of a country, for any reason," the coalition said. "Declaring war against a country is the most irresponsible thing a hacker group could do. This has nothing to do with hacktivism or hacker ethics and is nothing a hacker could be proud of," the coalition said in the statement. "Space Rogue" (of The L0pht), wrote, "Though we may agree with LoU that the atrocities in China and Iraq have got to stop, we do not agree with the methods they are advocating."

Date 1999-01-15 **Keyword** criminal hackers consultants white hat reformed business

Source, Vol, No. <http://www.upside.com/texis/mvm/news/story?id=369e739c0>

Deborah Radcliff reviewed some success stories — and some failures — for criminal hackers apparently gone legitimate. She interviewed famous (or notorious) formerly-criminal hackers Yobie Benjamin, Peter Shipley and barefooted Al Walker (Hobbit) as well as some of their employers and clients. The message in the article was mixed; some criminal hackers have failed miserably to adapt to the corporate world (and vice-versa) but a few are managing to convince at least some people in the business community that they may be trustworthy.

Date 1999-02-17 **Keyword** meta-hacking criminal script kiddies thieves Internet Web

Source, Vol, No. OTC

Script kiddies are increasingly being manipulated by meta-hackers — more experienced criminals who use the naïve kids to infiltrate systems and then collect information through their minions' activities. According to David Butler of Axent Technologies, "Cracking attempts rise by a factor or three or four during school holidays." New tools for meta-hacking include Java-based Trojans that can corrupt innocent users' browsers so that they inadvertently attack other Web sites and transmit information to the malefactors. In another meta-hacking attack, someone inserted code into the free Tcpwrapper software for authenticating logins; the Trojan version sent login records to an e-mail address. According to one of Nokia Telecommunications' marketing directors, Bob Brace, the company detected 24,000 cracking attempts between October 1998 and the end of January 1999. Many of the probes were spaced out over time in a stealth technique to avoid detection, said Brace.

Date 1999-02-22 **Keyword** criminal hackers Russia former Soviet Union fraud ISP

Source, Vol, No. Wall Street Journal

In Russia, criminal hackers were so active that many Net users lost control over their passwords and their accounts. Kimberley A. Strassel, writing in the Wall Street Journal, reported that several Russian police forces had formed cyber-police squads to patrol the Internet and help track down electronic thieves. A report in July 1999 suggested that a program code-named Moonlight Maze has been using criminal hacking techniques to steal military secrets from the US government and R&D data from US corporations.

Date 1999-04-01 **Keyword** criminal hacker punishment imprisonment protests pity

Source, Vol, No. Daily Telegraph

Wendy Grossman, writing in the _Daily Telegraph_ (1999-04-01), discussed the Kevin Mitnick case. She described how a relatively minor criminal hacker become the poster boy for a generation of criminal hackers and wannabes. Her closing remarks were particularly interesting: "The hacker community tends to follow the prison careers of all hackers and crackers as though they were political prisoners, and has rallied to support Mitnick, particularly as his time in jail without a bail hearing lengthened. The Free Kevin Web site (www.kevinmitnick.com) recounts every incident of his jail career, from his lack of access to legal books to the bizarre report that in early 1997 he was put in solitary confinement for unauthorized possession of 74 cans of tuna.
No one is saying it was all right for Mitnick to break into computer systems. But nothing he did was as destructive as Robert Morris's 1988 Internet worm, a badly written bit of code that paralysed large portions the network; Morris got probation. Equally, Mitnick is not known to have profited from information he copied, unlike some hackers who served lighter sentences. Finally, the general word about Mitnick is that he is not particularly a technical genius; his skill is in "social engineering" - persuading people to give him information they're not supposed to, such as passwords. Ultimately, what Mitnick's case and the publicity surrounding it have done is widen the gap of distrust between hackers and the law."

Date 1999-04-13 **Keyword** criminal hackers script kiddies children youngsters law enforcement detection tools penetration a

Source, Vol, No. AUSTRALIAN FINANCIAL REVIEW, Canberra Times

Script kiddies pose a worsening threat to the Net, according to ex-hacker Jeff Moss, now with Secure Computing. According to John Davidson, writing in the _Australian Financial Review_, Moss warned that the number of tools allowing know-nothing kids to hack successfully is growing; in addition, he said, law enforcement is falling behind in detection and prosecutions: "It's recently become very safe to use computers for crime. You really have to screw up, or you really have to attract the attention of the FBI for some reason, for there to be any negative consequences."

Date 1999-04-22 **Keyword** criminal hackers Y2K vulnerability attacks

Source, Vol, No. Computing (UK), Canberra Times

Many security experts warned that the Y2K transition could include a splash of criminal hacking. Stephen Cobb of Miora Systems Consulting and Neil Barrett of Bull Information Systems concurred that criminals would take advantage of the potential disruption due to non-compliant systems. In particular, everyone should be on the lookout for e-mail borne viruses and Trojans. Cobb warned everyone not to open e-mail attachments from strangers.

Date 1999-05-19 **Keyword** criminal hacker interviews publicity support

Source, Vol, No. Times of London

Morag Preston wrote a profile for the Times of London about the founder of AntiOnline, John Vranesvich. Mr Vranesvich was running his Web site about criminal hackers from the University of Pittsburgh when Ehud Tenebaum gave him an exclusive interview. When University officials forbade this use of their systems, he abandoned college and formed his own company. He admitted that his platform for criminal hackers runs the risk of glorifying activities which he dislikes (he is not a criminal hacker himself and says he has never approved of criminal hacking). He told Preston that he feels that showing kids the dangers of criminal hacking for both hackers and victims is an important educational message.

Date 1999-05-25 **Keyword** criminal hacker convention briefing conference

Source, Vol, No. PR

Secure Computing announced the 1999 Black Hat Briefings in Las Vegas for July 7-8. Participants included a mixture of security professionals and criminal hackers. Along with Peiter Zatko ("Mudge") of L0pht Heavy Industries and Peter Shipley (of 24-hour war-dialing fame) the platform included the respected cryptographer Bruce Schneier.

Date 1999-06-05 **Keyword** criminal hacker demonstration protest punishment excess justice

Source, Vol, No. Reuters

A dozen supporters of Kevin Mitnick protested his treatment by rallying before the US Supreme Court building in Washington, DC. They said they did not condone Mitnick's criminal hacking but felt that he was being punished excessively.

Date 1999-06-14 **Keyword** criminal hacker psychology biography history story adolescent teen-ager penetration gang tools s

Source, Vol, No. Wall Street Journal

John Simons of the Wall Street Journal wrote an extensive biographical sketch of Patrick Gregory, the 18-year-old who confessed to the FBI that he was "Mosthated," one of the founders of gH (Global Hell). The gH criminal hacker gang, with up to 30 members at various times, was one of the groups responsible for a wave of Web vandalism against US government and university sites in the Spring of 1999. The adolescent's story details how he became increasingly disruptive in school and finally quit school without graduating. He was arrested for possessing marijuana, lost his driver's license, and turned to full-time criminal hacking with a criminal hacker from Green Bay, WI who called himself Mindphasr. The two of the formed Global Hell and became involved in stealing credit-card numbers and abusing corporate conference-call lines. Gregory repeatedly broke into corporate systems, read internal e-mail, and vandalized systems. He then stupidly decided that a good way to get a job was to leave messages on the systems he penetrated telling administrators how to patch their security holes — so-called "gray-hat" hacking. He actually did get a job from one of his victims, Parachute Computing Systems of Austin, TX but blew it by continued criminal hacking in his spare time. He was busted by the FBI, which seized his computer. His mother immediately bought him another one and he was back online within a few days.

Date 1999-06-24 **Keyword** reformed criminal hacker security consultant trust doubt worry concern recidivist ethics

Source, Vol, No. Straits Times (Singapore)

Mathew Bevan was the subject of great concern a few years ago when he hacked into NASA, NATO and USAF computers systems. However, four years later, he describes himself as a reformed hacker and gives lectures on INFOSEC to anyone who will listen. Bevan, who was never prosecuted after his arrest at the age of 20, is now a security consultant who repudiates his past and dismisses the opinion of his erstwhile friends in the criminal hacker underground. Some of his clients expressed scepticism about his trustworthiness. Mr Sunny Tan of Singapore security company, Infinitum, asked, "Would you trust an ex-hacker with your network? He's done it once, he could do it again."

Date 1999-07-01 **Keyword** criminal hacker biography psychology corporate policy unauthorized use CPU cycles

Source, Vol, No. PC Magazine

Bill Machrone, veteran PC Magazine writer, prepared an insightful analysis of the Aaron Blosser case. Readers will recall that Aaron Blosser , a 28-year-old consultant, was accused in 1998 of misappropriating resources on 2585 computers at his client, U.S. West (a major telephone company). In his attempt to find ever-greater prime numbers, he commandeered over 10 years of processing cycles; as a result of the extra work, directory-assistance operators found the time for retrieval of telephone numbers stretching from the usual 3-5 seconds on into the 5 minute range. Associated Press reported, "The computers were so slow in mid-May that customer calls had to be rerouted to other states, and at one point the delays threatened to close down the Phoenix Service Delivery Center." Machrone wrote that US West declined to prosecute Blosser, who has learned his lesson: "Blosser ruefully suggests that anyone looking to do something with unused computer cycles on machines that are not their own ask permission first."

Date 1999-07-06 **Keyword** criminal hacker convention conference meeting

Source, Vol, No. South China Morning Post (Hong Kong), Birmingham Post (UK), Wall Street Journal

The annual DEFCON convention started in Las Vegas in early July 1999, complete with two camera crews filming the proceedings and interviewing criminal hackers after their presentations. Highlights (so to speak) included the release of BO2K, the new version of the BackOrifice program produced by the Cult of the Dead Cow in 1998. Along with the usual discussions of techniques used for criminal hacking, the convention featured various games such as Spot the Fed, Hacker Jeopardy (hosted by Winn Schwartau), various online games, a hacking contest, and wrestling in inflatable Sumo wrestler costumes. Some Federal officials actually spoke to the hackers (receiving some jeers at their suggestion that criminal hackers should join the good guys) and at least one security firm installed software on the hacker-target machines as a form of quality assurance: Ron Gula of Network Security Wizards, Inc. installed his intrusion-detection system on the target machines and was able to detect all attacks launched by the hackers, some of whom even suggested improvements to his program.

Date 1999-07-06 **Keyword** criminal hacker psychology biography interview

Source, Vol, No. Straits Times (Singapore)

The Straits Times (Singapore) published an interesting interview with some non-hacker observers of the criminal hacker scene in that country. Samuel Kwan, 16, and Nathanael Ng, 19, distinguished between honorable hackers and crackers, repeating the usual propaganda about intruders who leave polite messages indicating security vulnerabilities so they can be fixed. The young people sneered at "lamers" (aka "script kiddies") who use automated attack tools to cause harm but have no understanding of security or computer science.

Date 1999-10-13 **Keyword** criminal hacker collective subculture attitudes beliefs self-justification cult club gang

Source, Vol, No. <www.thesynthesis.com>

Someone calling him(or her)self "Bronc Buster" circulated a long description dated 1999-10-13 about a visit to the hacker collective New Hack City. The criminal-hacker supporter provides an interesting glimpse into the hacker underground, with hints of intrigue, elitism, and a time perspective that might startle adults: "New Hack, as the people who hang out there like to call it, was an idea that started way back in 1995 on the opposite side of the country, in Boston. It started with several friends wanting to find a place to gather, where they could share their experience with each other, learn, experiment, and most importantly pool their limited resources. In the early days of the Internet, as we know it, computer equipment was expensive, and dial-up access to it was hard to come by and was also expensive." The early days of the Internet? 1995? "So five people, FreqOut, GarbageHeap, ChukE, Rosie, and Deth Veggie, start the original New Hack City in Boston in 1995." The article continues with details of the links of this "hacker think-tank" with other criminal hacking organizations: "Many members of New Hack are also in the cDc, have been associated with the L0pht or worked with 2600. Regular people that hang out include a few people from the DOC, some people with 2600, and other notable groups. When I was there, several cDc members were there that are also part of the New Hack crew; like Tweety Fish, Deth Veggie and Sir Dystic (who wrote the original Back Orifice tool)."

Date 1999-10-29 **Keyword** hiring criminal hacker prison sentence probation job

Source, Vol, No. Australian Financial Review < http://www.afr.com.au:80/content/991023/inform/inform1.html >

In March 1998, Skeeve Stevens was sentenced to 3 years in jail but parole after 18 months. Stevens, aka "Optik Surfer," pleaded guilty to stealing and publishing 1200 credit card numbers belonging to subscribers of Australian ISP AusNet in 1995. In October 1999 he was released and immediately hired as a security consultant by June Heinrich, chief executive of Baptist Community Services. She was quoted as saying, "Well, he clearly was competent, wasn't he."

Date 1999-11-24 **Keyword** criminal hacker translation manual book instructions how-to guide children wannabe script-kiddi

Source, Vol, No. Bangkok Post

A report in the Bangkok Post in late November by Otto Sync stated that a well-known criminal hacker in Thailand published a Thai-language compilation of elementary hacking tools. Security experts should look for increased hacking activity from Thailand.

Date 1999-12-12 **Keyword** criminal hacker movies film plays style fashion sexy popular heroes villains journalists media ste

Source, Vol, No. New York Times

Jesse McKinley published an interesting review in the New York Times of the changing representation of criminal hackers in the popular media and entertainment. He pointed out that some of the early films from the 1980s (e.g., War Games, Hackers) showed hackers in a mostly positive light, whereas lately they have been shown as darker, sometimes flatly evil, characters.

Category 1C Pornography, Net-harm,cyberstalking, gambling (cases)

Date 1999-01-06 **Keyword** child pornography pedophiles Internet Web site prosecution

Source, Vol, No. Belfast Newsletter

Focus on Children, a Dublin-based charity, discovered a nasty nest of pedophiles operating a child-pornography exchange service on Web sites they found in mid-1996. In a 30-month investigation, the agency cooperated with the European Commission in Brussels and with police forces (including the FBI and Europol) to close in on the perpetrators.

Date 1999-02-23 **Keyword** hate speech Web report

Source, Vol, No. Reuters

According to a study by the Southern Poverty Law Center issued in February 1999, hate groups such as the KKK were using the Web as a cheap and effective way to twist the minds of victims, many of which were in colleges and universities. The spread of hateful speech through the Internet vastly increased the potential audience, said the SPLC.

Date 1999-02-24 **Keyword** gambling international regulation legislation supervision

Source, Vol, No. AAP

In Australia, a conference on casinos and gambling heard from the chair of the US Interactive Gaming Council, Sue Schneider, that an international interactive gaming council should be established to supervise online gambling. Chris Herde, writing for Australian Associated Press on 1999-02-24, wrote that the 1998 value of online gambling worldwide was several billion dollars a year and that the number of online gambling sites had risen from 15 in 1997 to more than 280 in 1999. [Of course, the entire online gambling industry is an IQ test: people who gamble online are willing to allow someone to take their money to allow them to bet on random processes simulated by computer programs. The victims of these potential or actual scams must be unaware that computer programs can generate non-random results as easily as pseudo-random sequences. In June 1998, for example, it was discovered that the Arizona state computer-based lottery had never in its history generated a number 9 in winning numbers. It is presumed that the error was due to quality assurance failures, but the same kind of problem could just as easily be deliberate.]

Date 1999-03-05 **Keyword** child pornography Internet pedophiles journalist law

Source, Vol, No. AP, USA Today via EDUPAGE

In 1998, freelance journalist Larry Matthews of Maryland was arrested for trolling through child pornography sites on the Internet in violation of federal laws. Although Matthews pleaded guilty to the felony, he argued that he was merely trying to investigate the problem of child pornography. The judge dismissed his argument and sentenced him to 18 months in a halfway house. Matthews planned an appeal.

Date 1999-11-15 **Keyword** child pornography police law enforcement crackdown investigation interdiction Internet

Source, Vol, No. The Times (London)

The British Home Office announced a feasibility study for the formation of a top-level unit dedicated to investigating and interdicting crime on the Internet. A particular focus of the team would be stopping the traffic in child pornography.

Date 1999-11-24 **Keyword** Web pornography libel nude picture pornography victim policy international

Source, Vol, No. The Nation (Bangkok)

Angkana Timdee and two other famous Thai actresses were furious when fake pictures appeared on an Internet Web site purporting to show them in the nude — a serious matter in Thailand but not in the USA, where the Web hosting company was presumed to be unaware of the fraud.

Date 1999-11-29 **Keyword** stalking harassment law enforcement Internet police investigation prosecution

Source, Vol, No. The Guardian

Duncan Campbell, writing in The Guardian (1999-11-29, p. 13), reported on the increasing threat of cyber-stalking. A new report by the Attorney General of the United States warned that obsessive stalkers are increasingly turning to the Internet as a tool in their campaigns of harassment. A couple of high-profile cases:

* Gary Delapenta was jailed for six years in July for having posted a young woman's address as that of a fictional sado-masochistic woman; at least six men tried to break into his victim's house. Delapenta was tricked into communicating with the victim's father, who trolled the Net looking for him and turned over enough evidence to the FBI to allow an arrest.

* Duwayne Comfort, a post-graduate student at the Catholic University of San Diego, CA was arrested after police set up a camera in the university computer lab to trace the sender of threatening e-mail messages to five women students. Comfort also hacked into the university records and lowered his victims' grades. Due to Comfort's need for a serious heart operation, he was given only a year's suspended sentence.

The US Department of Justice published a report in August on cyber-stalking; it was posted online at <http://www.usdoj.gov/ag/cyberstalkingreport.htm>.

Category 1D Theft of identity, impersonation

Date 1999-05-06 **Keyword** identity theft impersonation fraud credit card bank e-mail

Source, Vol, No. Globe and Mail (Canada)

Tyler Hamilton wrote a good review of identity theft in Canada's _Globe and Mail_ newspaper on May 6, 1999. The article included practical advice from Anne Cavoukian, Canada's Privacy Commissioner; excerpts:

HOW TO FOIL THE IDENTITY THIEVES

* Never send any personally identifying information in an E-mail. Look into buying encryption software that will ensure that the only eyes that see the message belong to the person you're E-mailing.

* When you go to a Web site, don't provide any identifying information, unless you and the business have established a trusting relationship. Banks, for example, are usually safe bets.

* Avoid chat groups and news groups, or at least use an alias when posting messages in these open areas on the Internet.

* Ask to be taken off commercial mailing lists.

* Ask your credit bureau to attach a "fraud alert" note to your records, meaning that any request to change or access information in your file must be followed up by a call to your home. If your credit bureau doesn't have a fraud alert service, ask why and explain its importance to the bureau.

* Finally, empower yourself on the Internet by buying privacy-enhancing technologies, such as "anonymizer" software. The software lets you surf the Web and engage in E-commerce transactions under a pseudonym without having to compromise your privacy.

Category 1E Law Enforcement & Forensics (technology, organizations, proposals)

Date 1999-02-18 **Keyword** police law enforcement Britain data sharing network

Source, Vol, No. COMPUTER WEEKLY (UK)

In February 1999, British police began implementing the Holmes2 system (Unisys' Home Office Large Major Enquiry System) to encourage data sharing by criminal investigators. The system was already a year late, and critics worried that without widespread acceptance and installation, the data repository and retrieval system would prove useless.

Date 1999-04-20 **Keyword** crime hacking international cooperation police investigation

Source, Vol, No. OTC

The Japanese National Police Agency announced formation of a national cyber-crime center. Japanese records suggest that Internet-related crimes rose 13-fold between 1993 and 1998. In Japan, unauthorized intrusion into computer systems is not a crime unless there is evidence of tampering. Such limitations show how little legislators understand about the fundamental issues of information security as enunciated by Donn Parker: confidentiality, control, integrity, authenticity, availability and utility.

Date 1999-04-27 **Keyword** Internet forensic tool Web police law investigation

Source, Vol, No. Sydney Morning Herald (Australia)

The Australian Securities and Investment Commission's new head of computer fraud investigations, Tim Phillipps, will oversee the development of technologies and procedures for tracking and prosecuting online offenders.

Date 1999-04-27 **Keyword** Internet Web fraud police commission government law

Source, Vol, No. Age (Melbourne)

The Australian government set up a special group to monitor and reduce fraud on the Internet. The Australian Securities and Investment Commission inaugurated its National Electronic Enforcement Unit, based in Sydney and led by Tim Phillips, an experienced fraud investigator in the financial services sector. Phillips said he would be working to improve the Australian legal system's definitions and punishments of computer crimes.

Date 1999-04-27 **Keyword** surveillance privacy e-mail ISP spying law enforcement

Source, Vol, No. AAP, AGE (Melbourne)

The Australian Security Intelligence Organization announced its intention to seek remote access to computer records of suspects being investigated. Mr Richardson said ASIO had not yet broken into computers using existing technology as that was not permitted under current legislation. "However, we have been able to access information in computers through search and enter warrants ever since we have had search and enter powers," he said. "The proposed amendments relate to remotely accessing data in a computer. It is not actually about necessarily putting a device within a computer. Under the proposed amendments we are allowed to interfere with a computer insofar as it enables us to compromise the protection mechanism that may surround the information in the computer. We are not allowed to interfere with the information in the computer itself or indeed the use of the computer."

Date 1999-05-03 **Keyword** information warfare government military hackers response

Source, Vol, No. IsraelWire

Israel announced formation of an information warfare unit combining elements of police and the military. The unit was tasked with providing intrusion detection and analysis, forensic support to law enforcement and damage control in the case of attacks on military, government or critical-infrastructure computers and networks in Israel.

Date 1999-05-03 **Keyword** police face identification software forensic tool

Source, Vol, No. Business Wire

InterQuest released 50,000 free copies of its FACES, The Ultimate Composite Picture tool to police forces and the public in the US and Canada plus 4,600 copies to forensic artists around the world. The tool has been hailed as a breakthrough in allowing rapid recreation of a suspect's face from a library of 4,000 facial elements. Victims have been able to produce photo-realistic composites within 10 minutes and the tool's successes have been featured on the FOX TV show "America's Most Wanted." For more information, see <http://www.facesinterquest.com>; phone 1-888-824-3223 or (450) 462-6886.

Date 1999-05-04 **Keyword** fraud hoax public education investment Web e-commerce

Source, Vol, No. AAP

The Australian Securities and Investments Commission (ASIC) posted a bogus investment scheme on the Web and snagged 233 investors who were willing to send money without any investigation whatever of the nonexistent company selling "millennium bug insurance." ASIC warned consumers not to invest in unknown companies without checking their bona fides.

Date 1999-07-01 **Keyword** government law response criminal hackers attacks Web vandalism legislation initiative proposal

Source, Vol, No. Newsbytes

The US House Committee on Science reactivated a proposal for better definitions of computer crime. Congress discarded a similar proposal, H.R. 1903, in 1998. This year's Computer Security Enhancement Act of 1999 upgrades the Computer Fraud and Abuse Act of 1987. Key points in the proposal would:
* encourage government agencies to comply with NIST security standards.
* encourage government use of commercial off-the-shelf (COTS) security products.
* require the Computer System Security and Privacy Advisory Board to propose standards and alerts about new INFOSEC issues.
* create a fellowship program for graduate and undergraduate students studying computer security.
* direct the National Research Council (NRC) to assess PKI systems.
* establish a national panel on a national digital signature infrastructure.
* require the Under Secretary of Commerce for Technology to enhance federal communications networks security.

Date 1999-10-01 **Keyword** psychological profiling geographical serial killers rapists criminals police investigation detection

Source, Vol, No. Detroit News, Independent on Sunday (UK)

Psychological profiling of serial killers and serial rapists is showing encouraging results worldwide. One of the leaders in the field is Bob Keppel of the Institute for Forensics in Seattle, WA (800 Fifth Ave., Suite 4100, Seattle, WA 98104; phone 206-447-1405).

Date 1999-10-04 **Keyword** law enforcement police sheriff children drugs gambling gun sales Web Internet crime child porno

Source, Vol, No. Detroit News

Sheriff Robert Ficano of Wayne County, MI set up an Internet Crime Bureau to deal with Internet-mediated prostitution, drug peddling, pornography, illegal gun sales, fraud, child pornography and pedophilia. The Bureau has successfully investigated many cases and arrested suspects. Irvin L. Jackson of The Detroit News ended his article with this list of recommendations for parents:
Here are some guidelines police, educators and online services say parents should follow when letting their children use the Internet (direct quote):
* Keep the computer in an open, easily accessible part of the house, where you can walk by and see what is on the screen at any time.
* Monitor your children's time online and keep a good idea of what sites they surf and what they are downloading.
* Make use of parental controls and software geared to keep minors out of inappropriate sites.

Date 1999-10-06 **Keyword** law enforcement police crime Internet Web child pornography fraud credit card

Source, Vol, No. Mercury (Hobart, Australia)

In the Netherlands, 15 "cybercops" began their Internet and Web patrols to identify and stop crime of all kinds. The Internet Police were set up with procedures for obtaining court orders allowing phone taps and cracking into suspects' computers in a search for incriminating evidence.

Date 1999-10-07 **Keyword** criminal hackers law enforcement investigation personnel resources

Source, Vol, No. AP, Xinhua

The head of the FBI's NIPC (National Infrastructure Protection Center) admitted that the agency is short-staffed in the computer-crime area. Testifying to the US Congress, Michael Vatis said that Washington, New York, San Francisco, Los Angeles and four other cities each had at least seven FBI agents trained in computer forensics; however, ". . . because of resource constraints, the other field offices have only one to five agents dedicated to working on . . . [computer intrusion] matters." According to Vatis, the FBI has 800 cases pending — double the load in 1997 and quadruple the load from 1996. The Director also acknowledged that the FBI was convinced that the "Moonlight Maze" hackers thought to have been involved in military espionage were from Russia. The next day, the Russian Foreign Intelligence Service denied having anything to do with Moonlight Maze.

Date 1999-12-01 **Keyword** stolen goods auction Web stupidity police e-commerce

Source, Vol, No. AP

Police have occasionally found that thieves are trying to fence stolen goods on Web-based auction sites. A few cases have occurred on eBay; in one episode of the Perils of Stupidity, someone posted a description of a tallit (prayer shawl) that had been stolen in October from a car in Baltimore. The victim scanned eBay looking for his tallit and other religious items and got help from police. An officer made the winning bid, got the address where the shawl was temporarily stored and got it back for the victim. Officials at eBay warned thieves that the service cooperates with police to crack down on the sale of stolen goods and even hires former prosecutors to scan the service and work with law enforcement to catch criminals.

Date 1999-12-07 **Keyword** Internet crime law enforcement detection evidence law

Source, Vol, No. Reuters

In December, Michael Vatis (Director of the FBI's National Infrastructure Protection Center, or NIPC) told a conference organized by the International Chamber of Commerce (ICC) that law enforcement was "seriously behind in tackling Internet crime" and warned that cybercrime could be a threat not only to businesses but also to nations. Brian Jenkins, an ICC advisor, listed what he called an "electronic bestiary" of cyber-criminals such as cyber-stalkers, identity-thieves, and money-launderers. Calling Internet fraud artists "locusts," he said, "They will infest e-commerce and are capable of consuming a great amount of wealth if unchallenged."

Date 1999-12-07 **Keyword** domestic surveillance privacy government NSA terrorism law enforcement cooperation

Source, Vol, No. Reuters, Washington Post

Newsweek magazine published an article in its December 13th issue claiming that the National Security Agency (NSA) intended to participate in criminal investigations with the FBI, especially where terrorism was suspected. The NSA categorically denied any intention to put Americans under surveillance in the United States. [This position did make it possible that domestic surveillance would be carried out on non-citizen residents of the US.]

Category 21 Quality assurance failures (general)

Date 1999-01-03 **Keyword** QA quality assurance bug spreadsheet data export import

Source, Vol, No. RISKS 20 14

A RISKS correspondent noted that exporting numbers with 12 significant figures from Excel to a comma-delimited CSV file and back causes loss of the last 5 significant digits -- and it doesn't even roundoff, merely truncates.

Date 1999-01-15 **Keyword** QA

Source, Vol, No. RISKS 20 15

Craig Raskin reported in RISKS that several Y2K testing tools missed obvious errors in test programs he devised for quality assurance of his own Y2K tools. He wondered how many errors such commercial tools are missing in the production environments where they are being used trustingly by Y2K-compliance teams.

Date 1999-01-15 **Keyword** Y2K QA quality assurance

Source, Vol, No. RISKS 20 15

James S. Vera wrote in RISKS 20.16: Intuit's Quicken'99 fails with a "divide by zero" message when a transaction dated in January 1999 is recorded in the Auto category and its "Home and Car Center" is opened.

Date 1999-01-29 **Keyword** QA Y2K quality assurance

Source, Vol, No. RISKS 20 18

In the southern Swedish city of Malmö, a new version of the municipal accounting package caused consternation by losing transactions every night when the system would crash. As a result, some bills were not being paid, causing embarrassment for the city and cash-flow problems for the unpaid vendors.

Date 1999-02-01 **Keyword** QA quality assurance failure bug underpayment contract

Source, Vol, No. RISKS 20 19

In England, the government's expensive (£140M) new NIRS 2 social benefits computer system installed by the UK Government Department of Social Security (DSS) was more than a year late in delivery. As a result, thousands of widows were underpaid for up to two years; missing amounts ranged from £1 to £100 a week. The government was therefore sitting on (and earning interest on) a windfall of £1B in unpaid benefits.

Date 1999-02-03 **Keyword** QA Internet Explorer Microsoft antitrust trial embarrassment

Source, Vol, No. Wired via PointCast

A huge gefuffle over a small error erupted in the marathon Microsoft antitrust trial. A videotape of how slowly Windows 98 would access the Web when modified as instructed by government attorneys and experts. Turns out the videotape was made correctly but installation and uninstallation of the software for access to the Prodigy value-added network damaged the system registry.

Date 1999-02-04 **Keyword** programming error bug array dimension limit rollover

Source, Vol, No. Investor's Daily, USA Today

As the Dow Jones industrial average approached 10,000 there were warnings that older software might rollover their interpretation of the index to 1000, causing a wave of automated selling and a potential dip in the stock market. In the event, nothing bad happened.

Date 1999-02-10 **Keyword** QA quality assurance misplaced faith technology records

Source, Vol, No. RISKS 20 20

At Carnegie Mellon University, Professor Philip Koopman lost his photocopier privileges for one of his graduate courses because the administrators reported, straight-faced, that he and his students had made 4,294,967,026 copies in two weeks. They knew this because a computer told them so. Prof. Koopman didn't even bother doing the page/minute calculations but commented that the number was suspiciously close to 2**32 and that it [was] far more likely the number -272 printed with an unsigned print format, but that argument didn't do [him]any good." He should have stuck to the page per minute calculation ((it works out to ~3551 copies per _second_ continuously for the entire 14 days).

Date 1999-02-12 **Keyword** quality assurance Web site correction privacy

Source, Vol, No. San Jose Mercury News

Hallmark Cards deserves kudos for fixing a security hole on its Web site within 5 minutes of the first alert. [Would that everyone were so responsive.]

Date 1999-03-01 **Keyword** QA quality assurance automated phone

Source, Vol, No. RISKS 20 23

Keith Rhodes wrote in to RISKS, "A police computer in Fort Worth TX made 1,300 phone calls to invite residents to a police community forum -- beginning at 3 a.m. Sunday morning, instead of during the day."

Date 1999-03-11 **Keyword** date quality assurance QA

Source, Vol, No. RISKS 20 24

Kenneth Dyke reported in RISKS that several improperly-dated e-mail messages caused confusion and disorder in his MS-Outlook in-basket. For example, a message dated "Sun, 4 Jan 2099 18:28:02 -0200" was listed by Outlook as being dated "Fri, Aug 1, 1919, 12:28 PM." This and other errors did not increase Mr Dyke's confidence in Microsoft's Y2K remediation programs.

Date 1999-03-11 **Keyword** availability crash rollover design quality assurance QA time

Source, Vol, No. RISKS, < http://support.microsoft.com/support/kb/articles/q216/6/41.asp > 20 24

Because of what appears to be a 32-bit millisecond counter in the Windows95 and Windows98 Vtdapi.vxd module, all Windows 9x computers hang after 49.7 days of continuous operation. [See <http://support.microsoft.com/support/kb/articles/q216/6/41.asp>]

Date 1999-03-11 **Keyword** prison jail doors locks open

Source, Vol, No. RISKS 20 24

ICSA.net's Director of Research Services, David Kennedy, wrote in RISKS, ". . . cell doors on the ninth floor of the Kenton County Detention Center in Covington KY opened spuriously and remained open for 9.5 hours, although the convicts were still confined within a larger area.

Date 1999-04-15 **Keyword** privacy confidentiality e-mail addresses prospects blunder error bug snafu QA quality assurance f

Source, Vol, No. CNET News.com <http://www.news.com/News/Item/0,4,35168,00.html>

Strike another blow for better quality assurance: registrants on the Xterra Web site run by Nissan were surprised to receive e-mail containing the entire list of 24,000 e-mail addresses of all those who had registered — a gold mine for unscrupulous scumbag junk mailers — or to competitors engaged in competitive intelligence. A Nissan spokesperson lamely explained that a "technical error" had done the deed. Yeeeessss, we had already deduced that the e-mail was unlikely to have been sent deliberately. . . .

Date 1999-04-15 **Keyword** privacy confidentiality e-mail addresses prospects blunder error bug snafu QA quality assurance f

Source, Vol, No. CNET news.com <http://www.news.com/News/Item/0,4,35225,00.html>

In April 1999, AT&T sent 1,800 e-mail messages containing all 1,800 addressees in the visible TO: field. Some recipients expressed concern about having their e-mail address distributed to junk e-mailers. A company spokesperson blamed human error for the blunder. In a story for CNET news.com, Troy Wolverston reported that, "Online privacy activist Jason Catlett, president of Junkbusters, said the Nissan and AT&T incidents show that companies are still trying to figure out how to use the Internet to target customers. He said that companies are starting to consider email to be an important marketing tool, but they lack the expertise to use it properly."

Date 1999-04-21 **Keyword** QA quality assurance browser bugs correction patches

Source, Vol, No. CNET News.com <http://www.news.com/News/Item/0,4,35492,00.html>

Microsoft responded quickly to serious vulnerabilities in its Internet Explorer browser versions 4 and 5 by issuing patches within a couple of weeks after revelations that malicious Web sites could bypass IE security mechanisms using misleading URLs. The weaknesses allowed access to user files and a simple mechanism for hijacking Web connections, putting up spoofs in place of authentic pages and thereby tricking users into revealing confidential information such as user IDs, passwords, credit-card numbers and so on. Another peculiar feature was corrected in IE 5, where it was possible for a Web page to force an executable ActiveX control into a user's clipboard.

Date 1999-07-19 **Keyword** Y2K programming quality assurance embedded code rollover time limits dates UNIX

Source, Vol, No. New York Times

A New York Times article reported on many date-related problems that will persist beyond the Y2K transition. For example, a well-known counter in UNIX systems rolls over to zero in 2038. Microsoft programs have counters that will break at various times; for instance, MS-Visual C++ will break in 2036 unless there are significant changes to the compiler and existing programs are recompiled before the limit. [In addition, many programmers have decided to use arbitrary windows of time rather than fixing the fundamental problem; thus they have defined two-digit ranges that fall into the 20th century and others that fall into the 21st. Unfortunately, no one agrees on precisely where the windows should lie so it is quite possible that an old product (or one based on an old product) will have serious problems in, say, 2025 whereas another one will break in 2030.]

Date 1999-07-21 **Keyword** financial fraud Y2K quality assurance outside consultants foreign study report

Source, Vol, No. Journal of Commerce

GartnerGroup issued a report on _Year 2000 and the Expanded Risk of Financial Fraud_ and warned that the huge effort to pry into production software worldwide has greatly increased the possibility that dishonest programmers will try to take advantage of the systems they have learned about — and modified, sometimes with minimal supervision.

Date 1999-07-21 **Keyword** liability tort Y2K protection law consumers

Source, Vol, No. Reuters

In July, the Clinton Administration approved a law to delay lawsuits against companies providing software or other products that are not Y2K compliant. The 90-day cooling-off period should allow repairs, according to supporters of the bill. However, opponents claimed that the delay would limit consumer rights. [Strike another blow for allowing companies to get away with making users serve as unpaid quality-assurance staff — and doing testing on production systems.]

Date 1999-07-30 **Keyword** Y2K quality assurance critical infrastructure protection government

Source, Vol, No. Reuters

The Y2K Information Coordination Center (ICC) was established by the US government with plans to go operational by 31 October 1999 and close down by June 2000. The Y2K-ICC would help coordinate government efforts in Y2K remediation and response and would also work with critical infrastructure to log and counter Y2K problems and possibly even cyberattacks. However, John Koskinen, chair of the President's Council on Year 2000 Conversion, told Newsbytes that the ICC would definitely not morph into the dreaded FIDNET (Federal Intrusion Detection Network).

Date 1999-08-21 **Keyword** GPS global positioning system rollover

Source, Vol, No. New York Times

The GPS time counter rolled over at midnight GMT on Friday Aug 20, 1999, with Saturday the 21st expressed as 0 instead of 1024 weeks since Jan 6, 1980. Although some people in Japan were inconvenienced by failure of their automobile GPS receivers, the event caused little disruption.

Date 1999-09-09 **Keyword** date problem glitch bug legacy code programs

Source, Vol, No. Philadelphia Inquirer

Some Y2K specialists were concerned about the possibility of legacy-code failures on 9-9-99 because that date used to be commonplace as a marker meaning "End of input data." However, almost no reports of trouble were publicized. Many observers hoped that this non-event presaged similarly mild problems over the Y2K transition.

Date 1999-10-01 **Keyword** malware backdoor Trojan logic bomb Y2K consultants sabotage infowar

Source, Vol, No. Newsbytes

Michael Vatis of the FBI's computer crime section and head of the National Infrastructure Protection Center warned that he expects to see significant sabotage and fraud carried out by consultants who have worked on Y2K fixes. The pressure and lack of quality assurance on outsourced program fixes makes his prediction reasonable.

Date 1999-10-28 **Keyword** quality assurance computer hardware bug flaw tort liability class action lawsuit settlement

Source, Vol, No. OTC

Toshiba announced in late October that it had settled a class-action lawsuit resulting from a bug in some of its laptops that allowed data corruption on diskettes when writing to the last byte on any sector. The company agreed to pay $2.1B in damages.

Date 1999-11-04 **Keyword** Web e-commerce sales preparation quality assurance load errors volume availability

Source, Vol, No. Wired

Handspring announced its new Visor palm-top computers and went online to sell them.
Unfortunately, the company failed to apply adequate quality assurance to its site and encountered so many problems that even its President couldn't get the units he ordered. Chris Oakes, writing for Wired magazine, described the debacle. Key points:
* The unexpected surge in Web and telephone orders caught the company unprepared.
* Few customers have received their handhelds.
* Some customers have received duplicate orders or been billed twice the right amount.
* The company has made errors in calculating the sales taxes.
* Their Web site crashed immediately upon opening for business because of the heavy demand.
* In response, the company hired 40 operators to deal with phone orders — and still had customers waiting two hours for service.
The author commented, ". . . Handspring has become a virtual case study in how not to conduct e-commerce."

Date 1999-11-29 **Keyword** Y2K QA quality assurance software testing bug glitch date

Source, Vol, No. Computerworld Online < http://www.computerworld.com/home/news.nsf/CWFlash/9911291jury >

Sami Lais, writing for Computerworld Online on 1999-11-29, described a Y2K glitch with wider import. In Philadelphia, Jury Commissioner Michael J. McAllister was surprised to find potential jurors reporting that they had received instructions to appear for jury duty on Jan 3, 1900. The Y2K-compliant jury-roster software had been cleared of date bugs during acceptance tests. Investigation showed that subsequent changes linked the program to a module in a non-compliant library.

Moral: all quality assurance tests must be repeated after any program modification before putting the new version into production.

Date 1999-12-03 **Keyword** quality assurance QA contingency planning glitches bugs errors failures

Source, Vol, No. <http://www.idg.net/go.cgi?id=203718>

Sean M. Dugan, senior research editor in the InfoWorld Test Center, published a thoughtful article in December about the implications of quality assurance for e-business. He pointed out that failing to have contingency plans in place to solve inevitable glitches is embarrassing and potentially disastrous for organizations trying to do business on the Web.

Category 23 Availability issues (not denial of service)

Date 1999-01-03 **Keyword** archives reference bibliography evanescence instability

Source, Vol, No. RISKS 20 14

An interesting article in RISKS DIGEST from correspondent Jerry Leichter pointed out that URLs are an unstable form of reference to scholarly work. He cited a case in which interesting papers disappeared from an academic Web site when the sponsoring research was disbanded. He also worried about using commercial sites as repositories for papers, arguing that the vicissitudes of the market make the destiny of such storage uncertain at best.

Date 1999-02-01 **Keyword** air traffic control critical infrastructure failure backup

Source, Vol, No. RISKS 20 19

Air traffic controller Paul Cox wrote in RISKS, "On 15 Jan 1999, at 2 PM, the power failed at Seattle Center, an en-route ATC facility that covers nearly 300,000 square miles of the NW United States." He described how the brief interruption in power during some routine tests set in motion catastrophic failure of the ATC in this area. Computers had to be rebooted, radar screens went dead for periods up to an hour and more, and the human controllers were frantic as they tried to shift planes from their normal 5 mile separation to the reequired 20 mile distances prescribed by the FAA. Luckily, the controllers had succeeded after much lobbying in having a backup radio system that did not require computers at all and that therefore worked at once after the power glitch. Mr Cox wrote, "This failure simply drives home yet again that backup systems are only as good as the main systems IF those backups are equally dependent upon a power supply. In fact, our backup communications system and backup radar display systems were essentially worthless to us, because they failed at the same instant as the main system did when the power died. As long as you have a single point of failure in any system, it doesn't matter how many backups you have downstream if they are dependent on that point."

Date 1999-02-01 **Keyword** emergency phone 911 system crash outage availability

Source, Vol, No. RISKS 20 19

On 1 Feb 1999, the New York City emergency phone system (911) crashed during a routine backup generator test. It seems the generator did not work and the backup system went down for an hour as technicians worked on getting the power generator running. The main system was down for six hours in all.

Date 1999-02-03 **Keyword** QA quality software down delay stop halt interruption broker

Source, Vol, No. Wired via PointCast; Washington Post

Installation of some new software on the ETrade Web-based stock brokerage caused intermittent, serious failures that interrupted electronic trading for several hours on Wednesday 3 February. Some customers interviewed by R. Scott Raynovich, writing for Wired, stated that they would pull their brokerage business out of Etrade for failing to provide consistent service. An anonymous investor reportedly said, "I'm trusting these guys with thousands of dollars of my money, and they can't provide me consistent access to it," said one ETrade customer, who asked to remain unnamed because he feared retribution from ETrade officials as he attempted to transfer money to another service. Hours, sometimes days, go by with me unable to put money into a suddenly hot stock, pull out of one that's tanking, or try to get in on an IPO. I'm disgusted with this company."

Date 1999-02-18 **Keyword** import availability down-time failure crash

Source, Vol, No. Wall Street Journal

John R. Emshwiller reported in the Wall Street Journal (" Customs Service's Old Computer System Triggers Worry," 1999.02.18) that the U.S. Customs Service's antiquated computers (antiquated in this era of Moore's Law means 14 years old in this case) are causing increasingly frequent failures of availability. Customs Service Commissioner Raymond Kelly said succinctly, "The system is collapsing." Random downtime causes backups in processing the flow of imports ($900B per year involving 19.4 million entry requests) with resulting delays in getting imported products to their destinations on time.

The most serious breakdown to date occurred on 1998.10.01, when hard disk failures caused a chain of system failures resulting in a six-hour downtime. The consequences were dramatic: a backlog of 80,000 requests. In a misguided attempt to stave off further electronic requests, system administrators shut down their modem lines; however, "many importers have automatic dialing systems that just kept resubmitting the requests, each of which was marked as a new entry." The Customs Service decided unilaterally to delete 45,000 of the accumulated requests, forcing resubmission for those shipments.

Currently, the Customs Service has requested financial support for new computer hardware and software, but the Clinton Administration has proposed paying for the $1B expense by levying an import fee -- a measure strenuously objected to by the business community, which would prefer funding from general tax revenues.

The article ends on a curious note: "One relative bright spot: Customs Service officials say they don't expect any major Year 2000 computer problems. On the other hand, said Woody Hall, an agency assistant commissioner, `the joke around here is that a lot of good it's going to do you to be Y2K-compliant if the system crashes around you.' "

Date 1999-02-24 **Keyword** availability online trading e-commerce failure crash

Source, Vol, No. AP

The Charles Schwab online stock brokerage computers went down at 09:37 on 1999-02-24 for about 90 minutes, causing disruption for its clients, who were normally placing an average of 153,000 trades a day online — 28% of the market for online securities trading.

Date 1999-03-01 **Keyword** availability interruption single point of failure downtime

Source, Vol, No. RISKS 20 23

On 21 Feb 1999, there was a 15 hour period when many ISPs in the UK were down due to (1) a problem on a transatlantic link maintained by Teleglobe and (2) the simultaneous upgrade of a mail server on the Cable Internet ISP. Malcolm Park noted in RISKS that many users of the affected ISPs complained about interference with their Net-dependent business. He pointed out that businesses should know that the Internet has no guarantee of service; at the very least, it would be appropriate for anyone dependent on the Net to have a contract with a backup ISP. [MK comments: here in Vermont, I have two ISPs -- and have often had to resort to the secondary one when the first one's local node is saturated or malfunctioning. Unfortunately, I still have only one set of wires between our home out in the boondocks and the central switch -- but at least the set includes three different phone numbers.]

Date 1999-10-06 **Keyword** contract fitness tort software license lawsuit date availability

Source, Vol, No. Financial Times (London)

In Italy, the clothing firm Industrie Zignago S Margherita sued UNISYS for refusing in 1994 to provide an upgrade to its System 1100 that would allow the ancient machines to cross the Jan 1, 1996 date boundary (presumably causing a date counter to roll over). UNISYS did offer a fix, but demanded payment. In October, the court ruled in favor of the client, saying that the supplier had violated its contract to provide software and hardware until 1997.

Date 1999-10-20 **Keyword** availability quality assurance load demand saturation crash encyclopedia reference

Source, Vol, No. Los Angeles Times

The Encyclopaedia Britannica opened its long-awaited free Web site, <http://www.britannica.com> — and immediately crashed because an order of magnitude more people tried to access the site than expected.

Date 1999-10-25 **Keyword** online file storage vault Web drive drop-box URL

Source, Vol, No. Wired < http://www.wired.com/news/print/0,1294,32051,00.html >

About 20 companies have announced free or cheap Web-based file storage for subscribers. One of the most aggressive marketers, i-drive, admits that it takes no responsibility for the security or legality of the materials stored on its servers. Privacy activists and security experts wonder about the safety of storing private information on someone else's systems; others expressed concern about the likely use of these services as ways of sharing stolen intellectual property. On the other hand, those services providing for legal storage and use of MP3 tracks, for example, would have a valuable source of market data for music companies.

Category 24 Mobile malicious code (JAVA, JavaScript, ActiveX; not assembly level or macro v

Date 1999-01-04 **Keyword** Java virtual machine applet corrupt crash Windows JVM

Source, Vol, No. Newsbytes

Fabio Ciucci and the Anfy Java Collective of Italy <http://www.anfyjava.com> warned in 1998 that weaknesses in Microsoft's "corrupt" version of the Java Virtual Machine made it vulnerable to applets that could crash client systems. Although Microsoft published a patch to correct the security hole, it did not publicize the patch. In January, Ciucci and his colleagues warned that the recent revision of the MS JVM [available from <http://www.microsoft.com/java/vm/dl--vm31.htm> or from <http://www.microsoft.com/windows/ie/download/jvm.htm>] were still vulnerable -- the company had failed to integrate the former patch in the new system. As a result, malicious applets -- increasingly available on the Net -- could cause incomprehensible JVM hangs and even outright crashes of the Windows operating system for users unaware of the need for a patch.

Date 1999-01-06 **Keyword** flaw spreadsheet Excel weakness HTML Web browser flaw

Source, Vol, No. InternetWeek <http://www.zdnet.com/intweek/stories/prtfriendly/0,4557,2182861,00.html>

A flaw in MS-Excel would allow malicious code written in HTML and downloaded from a Web site to execute arbitrary code secretly downloaded to the user system. The security hole would theoretically allow powerful violations of security such as sending confidential files to the hostile site. MS immediately provided a patch to disable the CALL function within Excel. Padgett Peterson, writing in RISKS 20.15, warned, "What is not well understood is that this exploit is actually multifaceted - there are a number of HTML constructs and a number of applications that can be used. The choke point seems to be in the (Windows) Registry which decides which applications (mostly Microsoft's) are considered "safe", that no warning screen is generated on network download/launch sequences for these applications. EXCEL is just one of these."

Date 1999-01-15 **Keyword** Java active content book publication Web mobile code

Source, Vol, No. RISKS 20 16

Drs Edward Felten and Gary McGraw published a new book about mobile code security. _Securing Java: Getting down to business with mobile code_ was published by John Wiley & Sons in January 1999. In addition to the physical book, these experts put the entire text online at <http://www.securingjava.com>. The hope was that the free edition will not harm sales of the paper book.

Date 1999-05-01 **Keyword** mobile active code ActiveX Java malware

Source, Vol, No. InternetWeek

Several companies announced products for identifying hostile or otherwise dangerous active content pulled from Web pages and executed on client systems. Finjan Software released a new version of its SurfinShield program; Security-7 announced a quarantine server for pre-emptive execution and validation of applets and controls. Experts warned that it is increasingly difficult to justify interdicting all Java, JavaScript and ActiveX execution because so many trading partners are depending on these tools for production Web applications. Rutrell Yasin, writing in InternetWeek, classified mobile code threats as follows:
* System modification: applets can exploit holes in Java, allowing hackers to alter database information;
* Privacy invasion: applets can be used to crack passwords or impersonate e-mail identities;
* Denial of service: applets can shut down a machine;
* Nuisance: applets can launch annoying attacks such as opening multiple windows.

Date 1999-05-10 **Keyword** mobile malicious code

Source, Vol, No. NATIONAL POST (Canada)

Edmonton computer expert Tom Cervenka, member of the vulnerability-tracking "Because We Can" group <http://www.because-we-can.com> identified a vulnerability in the Web site of e-Bay, a major on-line auction site. The vulnerability would allow a criminal hacker to insert harmful JavaScript code on an eBay Web page; the code could then do anything JavaScript allows, including password stealing. Unfortunately, eBay officials dismissed the vulnerability as unimportant.

Date 1999-08-03 **Keyword** Internet Explorer browser flaw weakness vulnerability bug macro execution Word Excel Powerpo

Source, Vol, No. New York Times via EDUPAGE

Because Microsoft believes that word processing, spreadsheet and presentation software should allow automatic execution of macros — thus turning these products into programming languages — they also allowed their Internet Explorer browser to load these programs without alerting users. In August, Microsoft scrambled to issue patches to correct this design flaw so that unwary users would not be subjected to hostile code merely by downloading documents from a hostile Web site or by reading e-mail attachments. The principle still stands: don't double-click attachments of uncertain origin or unvalidated safety.

Date 1999-09-29 **Keyword** MS-IE5 Microsoft Internet Explorer browser bug vulnerability ActiveX control download Web fi

Source, Vol, No. InfoWorld Electronic, IS/Recon, NTBUGTRAQ

Georgi Guninski, browser-bug discoverer extraordinaire, notified Microsoft of yet more security vulnerabilities in Internet Explorer 5. In August, he found that a malicious ActiveX control could install arbitrary code in the Windows Startup folder. See Guninski's Web site <http://www.nat.bg/~joro> for details but be aware that his demonstration code actually does subvert your security unless you set Internet Zone security setting to "High", or disable the setting "Script ActiveX controls marked safe for scripting." In September, he showed that a malicious JavaScript could download executable code from a Web site (typically allowed by firewalls) and the hostile code could then send itself to any IP address back out through the firewall. Microsoft recommended disabling IE5's active scripting.

Category 25 RFI, jamming (not interception), HERF, EMP/T

Date 1999-01-29 **Keyword** denial of service cellular phone signals control channel

Source, Vol, No. RISKS 20 18

In Crystal River, FL an innocent user unknowingly blocked all other cellular calls in his area whenever he used his new cell phone. The outages lasted 10 days while GTE tracked the problem down to his phone, which they replaced. [This case illustrates the vulnerability of the highly computer-dependent cellular-phone system to disruption -- accidental in this case but possibly deliberate in an information warfare attack.]

Date 1999-03-01 **Keyword** electromagnetic radiation interference HERF medical

Source, Vol, No. RISKS 20 23

A new digital TV station in Melbourne, Australia was assigned the same frequency as that used for heart monitors at the nearby Epworth Hospital. Specialists worried that the signals would interfere with output from the cardiac devices.

Date 1999-04-16 **Keyword** RFI radio frequency interference crosstalk

Source, Vol, No. Wired

Automatic garage doors in a six-mile (10 km) radius of the port at Hobart, Australia were shut down by the USS Carl Vinson's powerful 310-320 MHz communications transmitters — which happen to override the short-range electronic communications channel allocated by the Australian regulatory bodies for such devices as garage-door openers. In addition, one poor soul was unable to move his car when the transmissions overrode his car security system, locking the vehicle down until the huge ship left.

Date 1999-10-22 **Keyword** criminal hacker radio frequency interference RFI

Source, Vol, No. APB News

Someone drove around Boone County, KY setting off the warning sirens intended to alert the population to dangerous weather conditions. Although the sirens are supposed to sound for only a few minutes, attempts to shut them off met with resistance from the unknown prankster, who forced the racket to continue for up to 20 minutes. Since the sirens were to be used in cases of real danger such as approaching tornados, the prank could easily turn deadly.

Date 1999-11-30 **Keyword** electromagnetic radiation microwave cell phone memory brain

Source, Vol, No. RISKS, New Scientist, ABC News 20 23

Reports surfaced in March that cellular phone usage could be causing memory loss in mobile-phone users. Commentators expressed doubts about the veracity of this story from the London _Daily Mail_ because of sketchy details. However, a study with rats at the University of Washington (see <http://www.washington.edu/newsroom/news/1999archive/11-99archive/k113099a.html>) suggested memory loss for those critters in after exposure to cell phones radiation. A good review of the situation by David Concar appeared in the New Scientist on 1999-04-10 <http://www.newscientist.com/nsplus/insight/phones/mobilephones.html>. For more on this subject, see the following Web sites (links listed by Lycos):
<http://www.howstuffworks.com/cell-phone.htm>
<http://www.mcw.edu/gcrc/cop/cell-phone-health-FAQ/toc.html>
<http://www.drkoop.com/news/focus/july/cell_phones.html>
<http://www.goaskalice.columbia.edu/1428.html>
<http://www.electric-words.com/radiation/rindex.html>
<http://www.ecomall.com/greenshopping/magnet.htm>
<http://www.nrpb.org.uk/Nir-is4.htm>
<http://www.health.gov.au/arl/is_phone.htm>
<http://www.tassie.net.au/emfacts/mobiles/index.html>.

Category 26 Operating systems, network operating systems,TCP/IP problems (alerts)

Date 1999-01-12 **Keyword** bug time calendar operating system Microsoft Windows

Source, Vol, No. ZDNN <http://www.zdnet.com/zdnn/stories/news/0,4586,2186402,00.html>

In January 1999, Microsoft admitted that its Windows 95, Windows 98 and Windows NT operating systems contained a bug in the MSVCRT.DLL file that would delay the start of daylight savings time by a week on April 1 2001. The "April Fool's bug" would affect about 95% of all PCs in the world but should be fixed by patches that were posted on the WWW by Microsoft.

Date 1999-02-23 **Keyword** threats operating systems utilities vulnerabilities reports alerts

Source, Vol, No. CERT-CC Summary < http://www.cert.org/summaries/CS-99-01.html > 99 01

CERT Summary CS-99-01 (February 23, 1999) reported continuing threats from widespread scans, BackOrifice and NetBus, Trojan horse programs and FTP buffer overflows.

Date 1999-02-23 **Keyword** criminal hackers white-hat gray-hat Windows NT vulnerability hole

Source, Vol, No. OTC

What a newspaper writer called "The benevolent hackers of L0pht Heavy Industries" announced another Windows NT vulnerability. They warned Microsoft that editing the system cache would allow substitution of privileged DLLs by hacked versions that could do anything.

Date 1999-05-25 **Keyword** threats operating systems utilities vulnerabilities reports alerts

Source, Vol, No. CERT-CC Summary < http://www.cert.org/summaries/CS-99-02.html > 99 02

CERT Summary CS-99-02 (May 25, 1999) reported threats from new viruses, a resurgence of SYN flooding attacks, continued widespread automated scans and Web server attacks.

Date 1999-06-17 **Keyword** buffer overflow security flaw response publication patch

Source, Vol, No. LA Times

ECompany.com notified Microsoft of a serious (CERT-CC severity rating 95th percentile) security flaw allowing a buffer overflow to compromise MS Internet Information Server 4.0; vulnerabilities included complete access to all files on a server. The warning was apparently ignored, the tiny company published news of the problem and criticized the giant firm for failing to take security seriously.

Date 1999-07-26 **Keyword** buffer overflow UNIX calendar CERT-CC alert

Source, Vol, No. New York Times

CERT-CC issued an alert on buffer overflow vulnerabilities on several UNIX systems, including Solaris and HP-UX. Using this violation of memory array restrictions, criminal hackers can plant logic bombs and back doors on victimized systems. Manufacturers scrambled to provide patches.

Date 1999-08-31 **Keyword** threats operating systems utilities vulnerabilities reports alerts

Source, Vol, No. CERT-CC Summary < http://www.cert.org/summaries/CS-99-03.html > 99 03

CERT Summary CS-99-03 (August 31, 1999) reported threats and vulnerabilities from RPC, continued virus and Trojan horse activity, and continued widespread scans. In addition, the Summary provided information about the new CERT PGP key.

Date 1999-11-23 **Keyword** threats operating systems utilities vulnerabilities reports alerts

Source, Vol, No. CERT-CC Summary < http://www.cert.org/summaries/CS-99-04.html > 99 04

Topics in this regularly scheduled CERT Summary include distributed intruder tools and vulnerabilities related to CDE, BIND, WU-FTP, AMD, and RPC.

Date 1999-12-17 **Keyword** threats operating systems utilities vulnerabilities reports alerts

Source, Vol, No. CERT-CC Summary < http://www.cert.org/summaries/CS-99-05.html > 99 05

The CERT-CC issued a special edition of the CERT Summary. Topics included the Year 2000 and distributed-system intruder tools. The Summary also notified users of the new Current Activity Web page, "with a regularly updated summary of the most frequent, high-impact types of security incidents and vulnerabilities currently being reported to the CERT/CC. It is available from < http://www.cert.org/current/current_activity.html >.

Category 27 Tools for evaluating vulnerabilities

Date 1999-02-01 **Keyword** criminal hacker attack challenge revenge credit records

Source, Vol, No. RISKS 20 19

ICSA.net. has long warned vendors not to stage hacking challenges. These purported tests of security software are uncontrolled and teach little or nothing about the effectiveness of security systems. In January, Gen Technology, the maker of Access Denied network security software challenged hackers to break their system. Unfortunately, a criminal hacker who had boasted that he'd be able to crack the system within five minutes failed to break in at all. Enraged, the criminal then damaged the credit rating of Paul Smith, one of the software engineers on the development team, so badly that Mr Smith was precluded from receiving a home loan.

Date 1999-04-21 **Keyword** war dialer tiger teams commercial product vulnerability

Source, Vol, No. Business Wire

Sandstrom Enterprises Inc. of Cambridge, MA announced its commercial-grade war dialer, PhoneSweep. War dialers scan large numbers of phones for unauthorized modems; however, free hacker tools always pose a problem of quality and safety, since there's no guarantee that a criminal hacker has not inserted Trojan horse code in the software. See <http://www.phonesweep.com> for details.

Date 1999-11-20 **Keyword** scanner vulnerability audit tool WindowsNT firewalls intrusion detection

Source, Vol, No. InternetWeek

BindView Corp. and Network Associates announced their latest vulnerability scanning tools in November. Bindview's Hackshield 2.- and NAI's CyberCop Scanner 5.5 both announced new features such as better reporting and automatic repair of vulnerabilities.

Date 1999-12-01 **Keyword** password crack guess tool sniffer detection intrusion criminal hacker

Source, Vol, No. PC Magazine

The people at the L0pht announced two anti-hacking tools for modest fees. L0phtCrack provides efficient brute-force and dictionary-based analysis of network passwords; AntiSniff detects workstations that are configured in promiscuous mode to trap all network traffic in violation of normal security rules.

Prospective clients should be aware of L0pht's history. Their FAQ states that they are, "Just a bunch of hackers who got together and started working on projects together. One of the projects turned out to be L0pht.com. There are remnants of different groups that make up L0pht such as RDT, cDc, RL, etc. We didn't start this thing off to make money. We did this, and still do, out of a love we have for technology and making it do things that it might not have originally been meant to."

Their Web site features a FREE KEVIN logo and advertises an archive of files "especially useful to all Network Administrators, Hackers, Computer Security Professionals, Phreakers, Computer Teachers, Crackers, Lab Monitors, Virus Writers, Communication Specialists, and anyone else that wishes to have a copy of this unique archive collection for their personal use."

The members of L0pht continue to present themselves using their hacker handles; examples include "Mudge," "Weld Pond" and "Space Rogue."

Personally and professionally, I would no more run any of L0pht's products on a production system or a system connected to a trusted network or to the Internet than I would install BackOrifice written by cDc, the Cult of the Dead Cow) on such a system.

Caveat emptor.

Date 1999-12-03 **Keyword** vulnerability assessment scanner new version summary statistics

Source, Vol, No. InternetWeek

Axent Technologies announced release of its newest version of NetRecon (v. 3.0) with improved analytical tools and efficient, prioritized summaries of vulnerabilities.

Category 28 Denial of service

Date 1999-01-15 **Keyword** denial of service attack smurf e-mail saturation ISP Internet Service Provider

Source, Vol, No. RISKS 20 16

According to an article by Tim Barlass in the Daily Telegraph of Australia (12 Jan 1999, p. 9), someone launched a sustained Smurf denial-of-service attack on Ozemail, an important Australian Internet service provider. E-mail service has been disrupted for users in Sydney. A company spokesperson said they were trying to track down the perpetrator and were considering installing filtering software to prevent future attacks.

[Note from MK: a "Smurf" attack uses widely-available software written by criminal hackers to send ping packets with forged origination in the headers to a (usually major) corporate network's broadcast address. Every device -- perhaps hundreds or thousands -- sends a reply packet to the forged originator address. That system thus receives a flood of packets, often overloading its TCP/IP stacks and resulting in denial of service. See the article by Michael Dillon in ASK THE INFRA EXPERT (Internet World: Apr 20, 1998) for a more detailed explanation.]

Date 1999-02-12 **Keyword** security e-mail public access free

Source, Vol, No. USA Today

USA Today reported that HotMail and Yahoo, providers of free e-mail, were improving security by shutting down any account subject to several unsuccessful attempt to login. [MK comments: This is one of the oldest mistakes in system management, since it immediately opens each account to a trivially easy denial of service: simply try to logon several times to a victim's account without the right password and VOILA -- no further legitimate access until the account is reset.]

Date 1999-02-20 **Keyword** denial of service saturation operating system table UNIX

Source, Vol, No. RISKS 20 22

Simson Garfinkel, co-author with Gene Spafford of the classic text _Practical UNIX and Internet Security_, posted a serious warning of an unsolved vulnerability of UNIX (and other) operating systems: saturation of the process table. By launching a large number of TCP/IP connections on a target machine, an attacker can fill up the process table and thereby prevent the creation of any other processes while the table is saturated.

Date 1999-12-07 **Keyword** criminal hackers distributed denial-of-service attacks tools DDoS master slave

Source, Vol, No. Newsbytes

In August 1999, a new breed of automated attack tools surfaced in the computer underground. Trin00 and TFN were used to install slave programs on unprotected computers using Trojans to insert the unauthorized code. These slave programs, once loaded, wait passively for encrypted instructions from a master program. The slaves can then bombard a specific victim with a flood of spurious communications, causing a denial of service. Because many slaves respond to a single command from the master, the effects on a selected target can be devastating. This is a parallel processor for criminal hackers. Unfortunately, there is no simple fix for the problem; the ideal solution is to prevent the slaves from ever being installed by improving security on all sites on the Net — but don't hold your breath.

Date 1999-12-28 **Keyword** threats operating systems utilities vulnerabilities reports alerts distributed denial-of-service attack

Source, Vol, No. FedCIRC Advisory < http://www2.fedcirc.gov/advisories/FA-99-23.html > 99 23

FedCIRC and CERT-CC cooperated in summarizing the state of distributed denial-of-service tools at the end of December 1999. FedCIRC Advisory FA-99-23 reminded US government agencies that a variety of tools had been released on the Internet to amplify attacks on target systems, including the new TFN2K. In addition, MacOS 9 was vulnerable to serving as an amplifier for unwanted traffic with a ratio of 37.5:1 of output to input.

Category 29 Web attacks, vandalism

Date 1999-01-16 **Keyword** DNS reference pornography hijack URL 404 link

Source, Vol, No. RISKS 20 17

Daniel Tobias was startled to be criticized by a colleague who complained that his Web page included a link to a pornographic Web site. Indeed, one of Mr Tobias' originally inoffensive links did indeed now go to a porn site. The problem turned out to be a Web URL hijacking: the original owner of a domain either sold its domain to the pornographer or allowed the domain registration to lapse. The new domain owner programmed his Web site to link all references to the original pages at the original domain to point to his home page instead of returning a "404 Not Found" message. [MK comments: Net hygiene dictates that one check one's links regularly.]

Date 1999-01-21 **Keyword** vandalism Web attack damage Trojan Horse

Source, Vol, No. New York Times

The US Information Agency's Web site was severely damaged in January by vandals who installed Trojan Horse software.

Date 1999-02-12 **Keyword** Web server write-protect switch hardware

Source, Vol, No. RISKS 20 21

Electrical engineer Ian Cargill asked in RISKS why Web servers couldn't have hardware-based switches to prevent writing on the disks without authorization. It turns out that some hard disks do indeed have a write-protection jumper that could easily and cheaply be wired to an external switch. However, Nigel Rantor replied in the following issue that there were several problems with such a scheme: (1) Most Web sites have dynamic content that resides on the Web server (in part because many Web managers have no idea how to implement a back-end to a database on another server) and must therefore be in write-permit mode all the time; (2) many Web servers are hosted at third-party locations; asking for someone to flip a switch many times a day would be unacceptable. Mr Rantor also pointed out that even if the available methods for write-protection (firewalls, ACLs) are perfectly implemented, there are other ways of harming Web sites, such as denial-of-service attacks.

Date 1999-04-01 **Keyword** information warfare Web vandalism hacktivism April Fool's

Source, Vol, No. OTC

In a tasteless April Fool's joke (what other kind is there?), radio personality Art Bell's site on the Web claimed to have been hacked. The supposedly damaged site included text reading, "The Yugoslav Citizens' Message To Nato World Criminals" and urged worldwide protests against the NATO bombing campaign. Actually the site was altered by its owners in a stupid display of insensitivity toward people on both sides of a dreadful war.

Date 1999-05-12 **Keyword** criminal hacker Web vandalism

Source, Vol, No. OTC

The White House Web site was shut down for a day on 1999-05-11 after hackers attacked the server; NBC reported that the intruders left graffiti critical of NATO operations in Kosovo.

Date 1999-07-01 **Keyword** Web penetration vandalism political message criminal hackers

Source, Vol, No. InternetWeek

Criminal hackers vandalized the Web site of the State of Hawaii, leaving electronic graffiti with political statements on the damaged home page.

Date 1999-08-02 **Keyword** criminal hackers penetration Web vandalism hoax

Source, Vol, No. Newsbytes, Dow Jones, San Jose Mercury News

The Symantec Inc. Web site was hacked on 1999-08-01 and hoax claims of worm infection of the anti-virus company's products were left on the site. The hack was noticed by Dutch Symantec employees about an hour after the damage occurred. The company immediately notified the FBI.

Date 1999-08-03 **Keyword** criminal hackers penetration Web vandalism

Source, Vol, No. Newsbytes

A criminal-hacker gang calling itself HFD (Hacking for Drunks) vandalized the Jerry Springer Show Web site. The modified page included text such as, "Drunken hackers: The women who love them and the admins who fear them" and "On the next Jerry Springer... Meet beercan, b33rman, and beerb0ttl3. Three young men who have given there (sic) up their lives to alcohol abuse and computer hacking. They have agreed to come on Jerry to tell there story." Surprisingly, someone actually noticed that the subliterate, error-packed announcement of an ridiculous upcoming show was a hoax.

Date 1999-08-06 **Keyword** criminal hacker Web penetration vandalism

Source, Vol, No. AP

Someone using an IP address in Russia vandalized the anti-hacker AntiOnline site on 2000-08-05 by taking advantage of an unusual feature of the site. AntiOnline provides links to discussions taking place on other sites. Someone put executable code in a message that allowed the perpetrator to alter some links in the "Eye on the Underground" on the AntiOnline site. While the sabotage was unrepaired (about an hour), visitors clicking on the damaged link were shunted to a Web site showing an eye and the message, "Expensive security systems do not protect from stupidity." It was unclear whether the author of the message was making a self-reference or criticizing John "JP" Vranesevich, who had recently announced his intentions to aid law enforcement authorities in tracking and prosecuting criminal hackers.

Date 1999-08-10 **Keyword** international conflict information warfare INFOWAR hackers vandalism penetration Web sites g

Source, Vol, No. Wall Street Journal, Reuters

China and Taiwan extended their conflict over national identity into cyberspace in 1999, with hackers on both sides of the Taiwan Strait attacking each country's Web sites. Mainland hackers attacked Taiwanese Web sites with Chinese and English messages such as "Taiwan is indivisible part of Chinese territory and will always be! The Taiwanese government headed by Lee Teng-hui cannot deny it!" Taiwanese hackers penetrated Web sites of the China Securities Regulatory Commission and a Shaanxi government agency where they posted Taiwan's national flag and national anthem and messages such as "Go to the mainland to fight the Communists."

Date 1999-08-11 **Keyword** criminal hackers Web vandalism penetration

Source, Vol, No. OTC Newsbytes

The Federal Energy Regulatory Commission (FERC) Web site was vandalized on 1999-08-10 at 04:30 and was repaired by 07:00. The vandals posted a cartoon of a woman holding a whip and the words "Hacked by Sarin."

Date 1999-08-27 **Keyword** criminal hackers hactivists penetration Web site redirection hijack

Source, Vol, No. DataLounge Weekly News Recap

For a period of two days, the absurdly homophobic site <www.godhatesfags.com> was hijacked so that visitors to the hateful site were shunted to <www.godlovesfags.com>. As one commentator wrote, "While we can't applaud the hijacking of domains, we do appreciate the moral imperative that drove someone to temporarily replace a message of hate with a message of tolerance — and say in all sincerity that it couldn't have happened to a nicer bunch of folks."

Date 1999-09-08 **Keyword** criminal hackers Web vandalism racism government

Source, Vol, No. Newsbytes

The Level Seven Crew gang of criminal hackers, claiming 39 unauthorized penetrations of computer systems in 1999 alone, vandalized the Web sites of the US embassy in Beijing and the Federal Graphic Data Committee in early September. The embassy site's home page was replaced by a document containing racist comments about China and sneers and both the FBI and at other crmininal hacker groups.

Date 1999-09-15 **Keyword** criminal hackers Web penetration vandalism

Source, Vol, No. AP, Reuters, Wall Street Journal

A new criminal hacker gang calling itself "United Loan Gunmen" vandalized Internet gossip-monger Matt Drudge's Web site and then that of C-SPAN cable news network on 1999-09-05, leaving a badly-designed hoax claiming that the US government had conspired to foment conflict in the Middle East in 1983. The farce quoted "the Secretary of War at the State Department," a non-existent post. On the 15th of September, the same group attacked the Web sites of the NASDAQ and the American Stock Exchange. They left cybergraffiti claiming that they could have manipulated stock prices (apparently false) and that they had created e-mail accounts for themselves.

Date 1999-09-15 **Keyword** criminal hackers Web vandalism obscenity government

Source, Vol, No. Reuters

A criminal hacker gang calling itself "B1nary Outlawz"damaged the Web site of Statistics SA, leaving a page full of obscenities on screen instead of the usual consumer price data. Apparently the penetration occurred because of vulnerabilities in the Web hosting service provided by the SA Internet Exchange (Saix), a subsidiary of South Africa Telekom. There was initial suspicion that the vandalism might have been an inside job, as there was a labor dispute in progress at the time. This suspicion was not borne out by later evidence.

Date 1999-09-15 **Keyword** criminal hackers gang group attack penetration Web site stock exchanges vandalism

Source, Vol, No. Dow Jones, AP

The United Loan Gunmen criminal hacker gang vandalized the NASDAQ and American Stock Exchange in September. For Hallowe'en, the ULG vandalized the Associated Press Web site, leaving a greeting and a poem by Edgar Allan Poe on the home page.

Date 1999-10-05 **Keyword** vandalism Web attack defacement sabotage

Source, Vol, No. Straits Times (Singapore)

Three Singapore Web sites were defaced in early October by the criminal hacker calling him/herself "Mistuh Clean." The hacker blanked the home pages and left the electronic graffito, "owned…can we say more?" Local authorities wondered how they would proceed legally if the perpetrator turned out to be a foreign national living abroad. One mitigating circumstance is that the criminal may have been responsible for hacking into two US computer systems as well.

Date 1999-10-19 **Keyword** criminal hacker Web site penetration vandalism

Source, Vol, No. Wired < http://www.wired.com/news/print/0,1294,31986,00.html >

In October 1999, someone broke into the official Web site for George W. Bush Jr and replaced his picture with a hammer and sickle — the emblem of the Communist movement. To add injury to insult, the intruders placed links to the International Communist League on the vandalized page. The campaign's Web site is hosted on the Illuminati Online hosting service based in Autin, TX. Analysis by external security experts revealed that the Web site was basically unprotected against intrusion.

Date 1999-10-26 **Keyword** criminal hackers vandalism government Web damage Windows NT phreak.nl

Source, Vol, No. NEWSBYTES NEWS NETWORK

A criminal hacker or hacker group calling itself "phreak.nl" has been attacking US Web sites in the last week of October 1999. According to a Newsbytes article by Bob Woods dated 1999-10-26, the criminals damaged Web sites of NASA's JPL, the US Army's Redstone Arsenal's Program Executive Office and the National Defense University. All these sites were described by a hacker-publicity group, "attrition.org" as running WindowsNT servers. The defacements consisted of the usual puerile sneers and insults in the peculiar spelling affected by the criminal hacker subculture. One common theme was the notion that "phreak.nl" was engaged in "a game ... called hack the planet." In addition to these attacks, "phreak.nl" also damaged sites for All Timeshare, Pet GBets and WPYC. Anyone wishing to see copies of the damaged sites can do so at <http://www.attrition.org> but readers are urged to use caution when visiting any such site. Don't run active content, don't allow cookies and use a firewall on your workstation to preclude unauthorized activity.

Date 1999-11-01 **Keyword** criminal hackers Web vandalism prank satire government ministry

Source, Vol, No. AP

Criminal hackers penetrated the Web site of the Romanian Finance Ministry. The cybervandals left satirical content introducing taxes on stupidity and laying out an official plan to bribe NATO so that Romania could enter the military alliance quickly. There were no laws in Romania making such unauthorized activities illegal.

Date 1999-11-14 **Keyword** criminal hackers Web site defacement vandalism government

Source, Vol, No. Newsbytes

Several incidents in November reminded the world of the ongoing problems with hacking in Asia. A HK government website run by the Highways Department was trashed; the Chinese Ministry of Foreign Affairs suffered a similar indignity, with replacement of the home page by a blank screen with a few criminal hacker boasts and obscenities. In a related story, China announced that a former bank employee, Zhao Zhe of Shanghai, was sentenced to three years in prison for breaking into the computers of the Shanghai branch of a Hainan securities firm and altering share prices in a failed stock-manipulation scheme. In Singapore, criminal hackers defaced the Web sites of The Singapore Government Shopfront and the Ministry of Law's Integrated Land Information Service (INLIS) Web site.

Date 1999-11-16 **Keyword** Web vandalism attack penetration defacement court conviction sentencing

Source, Vol, No. Straits Times (Singapore)

In September 1999, someone calling him/herself "mistuh clean" vandalized the Web site of Mediacity, part of the Television Corporation of Singapore's network. Evidence suggested that the criminal hacker might not be a local but rather a foreigner, possibly a Canadian resident. The criminal contacted Victor Keong, a Canadian security consultant using e-mail to inform him of the vandalism, and Mr Keong called Mediacity to warn them of the tampering.

In November 1999, eighteen-year-old student Edwin Lim Zhaoming admitted having broken into the Television Corporation of Singapore (TCS) website on 15 June with the help of a Burmese confederate aged 15. Among other damage, the vandals renamed the site "Mediashity." The juvenile confederate who told him about an easy user-ID and password to penetrate the site was sentenced to 12 months probation and 100 hours of community service. The attack consisted of replacing the TCS Web site with a page larged with vulagarities and abusing Bill Gates; the company estimated that the site was down for 10 hours, took 80 person-hours and cost S$13,000 to recover .

Date 1999-11-18 **Keyword** Web site government vandalism criminal hacker defacement

Source, Vol, No. Reuters

In Belgium, (a) criminal hacker(s) vandalized several government Web pages, putting offensive messages about a local libel case onto the welcome pages at the Treasury and for an administrative court. Officials claimed that security on those Web pages was low because the information was public. [Come again?]

Date 1999-11-18 **Keyword** criminal hacker Web penetration vandalism

Source, Vol, No. Reuters

A criminal hacker penetrated the Web sites of the Belgian Treasury and of an administrative court in mid-November. The intruder put up obscene language referring to the legal case in which fashion designer Ann Demeulemeester succeeded in preventing distribution of a satirical book by Belgian writer Herman Brusselmans in which she was named.

Date 1999-11-20 **Keyword** Web vulnerability criminal hackers vandalism government

Source, Vol, No. Newsbytes

A rash of exploits using Remote Data Service (RDS) allowed criminal hackers to deface several US government Web sites in November, including the Department of Energy (DoE), Federal Aviation Administration (FAA), the National Institutes of Health (NIH), the National Oceanic and Atmospheric Administration (NOAA) and the US Postal Service (USPS). Damage included graffiti in some cases but wholesale replacement of entire pages in others.

Date 1999-12-07 **Keyword** criminal hacker Web site redirection information warfare lawsuit John Doe

Source, Vol, No. UPI, OTC

On 1999-10-09, someone breached security on the Staples Web site and redirected browsers to the Web site of Office Depot, the victim's major competitor. On 1999-11-30, Staples announced on that it filed a federal "John Doe" lawsuit against its assailant(s) claiming damages for lost business and for the recovery effort. Staples and Office Depot both said they doubted that Office Depot was in any way responsible for the attack.

Date 1999-12-07 **Keyword** Web vandalism criminal hackers

Source, Vol, No. Business Day (Johannesburg, RSA) via OTC

The criminal hacker group calling itself "B1nary Outlawz" attacked the Web sites of the South African Police Service and about a dozen other Johannesburg-based Web sites. The vandalism included obscenities directed at the police; the criminals notified the press through e-mail. The same group claimed responsibility for damaging the Web site of the Statistics SA department in September. In an apparently unrelated hack the Statistics department was hacked from a US address in November.

Date 1999-12-12 **Keyword** criminal hackers hactivists political propaganda Web penetration vandalism government

Source, Vol, No. ITAR-TASS, Reuters

Criminal hacker gangs calling themselvs "The Princes of Darkness" and "The Angels of Freedom" penetrated the Web site of the official Russian ITAR-TASS news agency. The intruders posted verbiage protesting the warn in Chechnya.

Category 2A Firewalls & other perimeter defenses

Date 1999-02-18 **Keyword** personal firewall PCs intrusion detection

Source, Vol, No. PR

Signal 9 Solutions of Kanata, ON (Canada) announced its ConSeal PC Firewall in February 1999, claiming that it was "the first firewall designed especially for the individual Internet user/surfer and SOHO small office/home office." [This news came as a surprise to users of products such as AtGuard from Walker, Richer & Quinn, released more than a year earlier.]

Date 1999-02-23 **Keyword** partition separation classified unclassified tunneling access-control firewall

Source, Vol, No. Australian

Dr Mark Anderson of the Australian Defence Science and Technology Organisation (DSTO) won the Minister for Defence Achievement Award for his development of the Starlight suite of INFOSEC products. The Starlight products allow secure access to unclassified systems on a workstation that includes classified systems and also an intrusion-detection system called Shapes Vector.

Date 1999-02-24 **Keyword** firewall configuration tips hints suggestions policies

Source, Vol, No. OTC

Finnish telecommunications company Nokia shared some of its INFOSEC recommendations in February 1999. Some of the key points:
* disallow pings outright: drop them entirely without any response.
* log everything coming into the firewall.
* configure NAT (network address translation) to drop ICMP packets without response.
* use the stealth rule: drop (not reject) any packet directed to the firewall (as opposed to the network inside).
* use VPNs where possible and re-authenticate users before granting access to restricted areas of the network.

Date 1999-04-13 **Keyword** firewall secure Web server criminal hackers

Source, Vol, No. PR

In an odd bit of publicity, Systems Advisory Group Enterprises, Inc. (SAGE) announced in April 1999 that Carolyn Meinel, a criminal-hacker sympathizer much detested by criminal hackers agreed to use the BRICKHouse(TM) Web server to protect the new Happy Hacker Web site <www.happyhacker.org> from hostile attackers.

Date 1999-08-03 **Keyword** personal firewall filtering home computer PC workstation intrusion-detection

Source, Vol, No. Business Wire and <www.networkice.com>

Network ICE launched its new personal firewall in August 1999. BlackICE software was described as suitable for home computers, especially those connected via cable modems, to block attacks from criminal hackers. The detailed log files serve the intrusion detection function by providing useful forensic evidence of the attacks. The company's press releases stressed the following features:
* Corporate strength intrusion defense for the consumer market.
* Runs on Windows 95, Windows 98, and Windows NT operating systems.
* Protects against over 200 signatures or known attacks such as Back Orifice, Smurf attacks and port scans.
* "Instant On" installation for quick and easy start up
* Intuitive user interface details hacker identification, intrusion severity level and attack summary
* Live alert mechanism for instant Internet attack notification
* AdvICE link for quick help and detailed information on Internet hacks

See <http://www.networkice.com> for more information. Cost of a one-year subscription was $40.

Date 1999-09-27 **Keyword** DSL cable modem ISP firewall

Source, Vol, No. PR

The Texas ISP Texas.Net announced that its DSL and cable modem users would not require individual firewalls, claiming that its own firewalls would do the job of protecting them against intrusion and damage.

Date 1999-11-17 **Keyword** virtual private network HTTP tunnel bypass firewall

Source, Vol, No. Network News, GNU

The NoCrew hacker group presented the world with HTTPTunnel, a tool to create an encrypted bi-directional data path that can elude firewalls and break policy on connections into and out of corporate networks. Writing in a firewalls discussion list, Stevin Bellovin wrote, "Firewalls are based on two fundamental assumptions: that anyone on the outside may be bad, and that all actors on the inside are good. If the latter assumption is false, your firewall is useless. Once upon a time, the inside "actors" referred to people. In an era of mobile code -- mobile in the sense of both Java/ActiveX and in reference to outside code that is installed -- the word refers to the such programs as well."

He continued, "Here we have a piece of `malware' -- code designed to subvert administrative policy. Although perhaps in theory it could be installed by, say, a Makefile in some popular package, or by a Trojan horse in something you run, most likely it would be deliberately installed by someone who doesn't like the firewall. But the difference isn't that important -- what matters is that either is a bad actor on the inside. The precise tunnel chosen isn't that interesting, either. . . . *Any* bidirectional channel can be used as a tunnel -- and if your users are hell-bent on getting around your firewall, they're going to. *Maybe* you can use traffic analysis to find such things, but then you're in a serious arms race. You can't use technical means to enforce a stricter security policy than your organizational culture will support, though human means, such as a chat with management, may work."

Category 2B Intrusion detection systems

Date 1999-02-18 **Keyword** intrusion detection software log alert warning penetration

Source, Vol, No. OTC

Internet Security Systems (ISS) has launched a new enterprise threat management system. The RealSecure 3.0 software detects attacks on both network and system levels and responds to any attack automatically. The product includes new detection methods for the latest kinds of attacks, including back door attacks, denial-of-service attacks and other unauthorized access methods. Customers will also receive updates about new uncovered threats.

Date 1999-03-16 **Keyword** intrusion detection protocol standards

Source, Vol, No. <http://www.nwfusion.com/news/1999/0316security.html>

The IETF working group on intrusion detection proposed a new scheme, the Intrusion Detection Message Exchange Protocol (IDMEP), for sharing information about attacks on systems and networks. Using the standard message formats, any participating system could automatically send messages describing the attack type and relevant addressing information.

Date 1999-04-10 **Keyword** security product coordination intrusion detection error firewalls reporting paging alerts warnings

Source, Vol, No. OTC

Network Associates announced a product for handling trousers: "Event Orchestrator, a security technology that enables products and tools from third-party vendors to coordinate responses to security breeches." Oh wait, that's probably not trousers; they meant security _breaches_. According to the puffery, Event Orchestrator is an object technology based on the Component Object Model that maps a company's security policies to actions," says Zachary Nelson, VP and general manager for Network Associates' Service Desk product line. It picks up alerts from security tools, checks the events against company policies, then takes appropriate action based on the level of risk. For example, if Network Associates' CyberCop Monitor detects a hacker attack, Event Orchestrator can order the ports on a firewall closed to block access rather than page a network administrator to do the same. "Properly configured, Event Orchestrator can react far faster than I can," says Christopher Ward, director of corporate security for Pagemart Wireless Inc., a wireless paging company in Dallas. The system can help to make different components of the security architecture work more smoothly together, especially when the configuration of one device, such as a firewall, can have an effect on others, such as anti-virus products.

Date 1999-04-13 **Keyword** intrusion detection White Paper Buyers' Guide product terminology standards descriptions selecti

Source, Vol, No. Business Wire

ICSA.net convened the Intrusion Detection Systems Consortium in April and presented a White Paper clarifying the concepts and standardizing the terminology used to describe intrusion-detection products (see < http://www.icsa.net/services/consortia/intrusion/intrusion.pdf >). In December they published a free (with registration) Buyers' Guide to Intrusion Detection.

Date 1999-04-21 **Keyword** intrusion detection product perimeter defenses

Source, Vol, No. Business Wire

CyberSafe Corporation announced Centrax v 2.2 intrusion detection software they describe as "the first and only product to integrate host- and network-based intrusion detection, vulnerability assessment, and policy management under a single, easy-to-use interface." See <http://www.cybersafe.com> for more details.

Date 1999-06-14 **Keyword** slow port scan bypass intrusion detection criminal hacker data diddling deletion malicious penetr

Source, Vol, No. Computerworld

In early 1999, a criminal hacker called "Moof"went on a rampage against Linux servers in a wide range of ISPs and colleges in the US, the UK and Canada. The cracker was using a "slow port scan" in which a probe packet gets sent one port at a time — one port every three hours. Such slow scans are not picked up by intrusion-detection systems, which tend to roll over their detection stacks every 10 minutes or so. In addition, the criminal uses different source addresses for different packets to make it even harder to detect the port scan. Once "Moof" had identified vulnerabilities, (s)he attacked the vulnerable system, installed back doors and used the compromised system to launch more slow scans for new victims. Finally, the criminal erased crucial file system entries on the latest victim, making the system crash.

Date 1999-08-03 **Keyword** intrusion detection response unauthorized modification digital signature

Source, Vol, No. The Australian & < http://www.creative.com.au/cdt_prod/securepage.html >

Creative Digital Technology (CDT) announced a system of digital signatures for Web servers that would allow the server instantly to stop supplying a hacked page. Unauthorized modifications of any kind to a signed Web page would be detected by the security software and the content blocked so that no one could receive it. More important, the software would substitute a copy of the original, unmodified, Web page from a strongly-encrypted cache. The company showed a responsible attitude towards open quality assurance by offering a cash prize — but only to universities — for the first computer scientists and students who could demonstrate a vulnerability in their system. See <http://www.creative.com.au/cdt_prod/securepage.html> for more information on the SecurePage product.

Date 1999-08-14 **Keyword** information warfare surveillance intrusion detection penetration analysis government FBI FIDNE

Source, Vol, No. National Journal

Neil Munro published a thorough review of the politics of the FIDNet (Federal Intrusion Detection Network) proposal in the _National Journal_ on 1999-08-14. The furore over the monitoring plans included opponents not only from the civil liberties camp but also, in an unlikely combination, representatives of high-tech firms. Companies expressed horror at the thought of mandatory reporting of computer crime because they mistrust the government's ability to safeguard their information and fear of ridicule and embarrassment if the truth were to be revealed to the public. In addition, people with libertarian tendencies just plain dislike government regulation of _anything_.

Date 1999-08-29 **Keyword** information warfare surveillance intrusion detection penetration analysis government FBI FIDNE

Source, Vol, No. New York Times, Washington Post, Wired

The privacy community was not pleased when the Clinton Administration and the FBI announced their FIDNET initiative in July 1999 to monitor network intrusions not only on government systems but also critical infrastructure components such as banking, communications and transport. House Majority Leader Dick Armey (R-TX) attacked the FIDNET proposal and the House Appropriations Committee removed funding for the project from its versions of the relevant appropriations bills. In August, one of FIDNET's main architects spoke out in defense of the plan. Richard Clarke, National Coordinator for Security, Infrastructure Protection and Counterterrorism, explained that fears of an "electronic Pearl Harbor" (a term popularized by Winn Schwartau of <infowar.com> in the early 1990s) led to Presidential Decision Directive 63 and that FIDNET was one of the first major computer-security programs proposed in response to the Directive. He assured skeptics of minimal involvement of the FBI and said that FIDNET would be managed by the NIPC (National Infrastructure Protection Center), not the Department of Justice. The system would not intrude on personal or corporate privacy, he said. On 27 Sept, Rep. Armey sent another challenge to the Dept of Justice demanding clarification of critical elements of FIDNET. In January 2000, the Administration tried again, bundling FidNET into anti-cybercrime proposals presented by the Department of Commerce.

Category 2C Addiction, cyber-syndromes, sociology

Date 1999-02-03 **Keyword** virtual reality sickness neurological damage perception VR

Source, Vol, No. EE Times via CMP News via PointCast

Michigan State University researchers found measurable neurological effects from prolonged exposure to virtual reality systems. Doctors using VR systems to gain information about a patient's anatomical details during knee surgery took 10 minutes to adapt to the slight spatial displacement of the image from the real knee; however, the distorting neuromuscular coordination effects of the head-mounted display units lasted 30 minutes after the doctors removed the VR rig.

Date 1999-02-20 **Keyword** Internet stalker harrassment junk e-mail fantasy violence

Source, Vol, No. Guardian (UK)

A survey by Novell in Britain revealed that "58% of men and 41% of women who use the Internet have been persistently stalked on it." An article in the Guardian newspaper by Sara Hall reported that the problem is exacerbated by the large number of new users who do not know enough to conceal personal information in public forums on the Net. Secondly, the large number of users means that the tiny percentage of weirdoes now constitute a significant number of people who harass others.

Date 1999-03-15 **Keyword** computer ethics government program proposal

Source, Vol, No. AP

In March, Janet Reno encouraged government and industry to work on teaching ethical behavior in cyberspace. [I call it integrating cyberspace into children's -- and our own -- moral universe.]

Date 1999-04-03 **Keyword** virus writers sociology psychology studies motivation

Source, Vol, No. NEW YORK TIMES NEWS SERVICE

Sarah Gordon, a respected anti-virus researcher working for IBM, commented that malicious code is all over the Net: "It's like candy - a child can get these, a 12-year-old can get these. It's trivial," she said. "All you do is download it to a computer, click on it, and there you go." Evidence supports the view that a growing number of virus writers and distributors are juveniles. On the other hand, some virus writers protest what they describe as simplistic generalizations. One fool going by the pseudonym "Attitude Adjuster" wrote, "The idea that all of us out here are malicious teen-agers is quite a fallacy. There are those of us who still exist in the community who write viruses because it's fun. We don't give our viruses to the public and nobody gets hurt."

Date 1999-09-27 **Keyword** geek nerd computer fanatic hacker syndrome psychology

Source, Vol, No. LA Times

Gary Chapman published an interesting article in the LA Times suggesting that some fanatical users of computers calling themselves "geeks" or "nerds" (or maybe "hacker") may in fact have symptoms of clinical syndromes similar to some forms of autism. Specifically, writes the author, "Unlike classic autism, which often involves mental retardation and a lack of verbal skills, Asperger's syndrome is at the `high functional' end of the spectrum of autistic behavior, experts say. People with Asperger's syndrome have normal or above-average IQs and may even display savantism, or exceptional abilities in a specific skill. What they lack is human empathy, a deficiency sometimes called `mind-blindness,' which shows up as a distinct inability to read routine human nonverbal cues of attitude such as kindness, anger or love. Asperger's syndrome patients, who usually develop their traits at a young age, often have these tendencies: excellent rote memory; fascination with fantasy worlds and arcane facts; facility with math and science; physical awkwardness or clumsiness and sometimes an unusual gait; hyperactivity but with an ability to focus on interesting problems for hours at a time; poor social understanding; hyper-verbal activity but without the ability to make contextual connections in conversations; and an appearance of insensitivity and eccentricity. They are commonly victims of teasing in school. And, apparently, some can do well in the computer world." However, some experts in the field claim that such interpretations are bunk, pointing out that most Asperger's Syndrome kids are severely debilitated.

Category 2D Port scanning

Date 1999-10-11 **Keyword** scanning probing proxies

Source, Vol, No. SANS < http://www.sans.org/newlook/resources/ringzero.htm >

Widespread port scans were reported in late September to the System Administration, Networking, and Security (SANS) Institute, which coordinated the effort to analyze the problem. Results: someone has probably distributed a Trojan Horse running under Windows that scans ports 80, 8080 and 3128 (and sometimes other ports in the 8000 range) for proxies. SANS advised system administrators to watch for outbound traffic for the target ports. Admins should also either disable unused ports or set firewalls to preclude proxies from being used by outsiders.

Category 31 Surveys, estimates

Date 1999-01-08 **Keyword** criminal hacker statistics survey report China international

Source, Vol, No. Newsbytes

The official Xinhua news agency reported that computer crime has been exploding in the People's Republic of China. The annual growth rate of 30% led to over 100 recorded cases of computer-related crimes in 1998 with estimates of undetected crime running about 6:1, with a projected rates of 600 crimes in 1998 in the PRC. One Chinese estimate guessed that 95% of all PRC Web sites have been penetrated by local and overseas criminal hackers because of the relatively weak level of security in the PRC. A test of Shanghai and Shenzhen networks showed that almost all of them were vulnerable to penetration. Local software companies are beginning to respond to the need for security software, and in late 1998, an anti-virus company announced the release of the first firewall made in the PRC.

Date 1999-02-18 **Keyword** computer crime penetration data diddling Japan survey

Source, Vol, No. OTC

In Japan, the National Police Agency reported in February that computer crime was up 58% in 1998 compared with 1997 — a 1300% growth since the first statistics were kept in 1993. Specific crimes increased even more than the aggregate average; e.g., forgery and data diddling cases grew 67% in 1998. Current Japanese laws do not consider unauthorized penetration of a computer system as a crime; only breaches of data integrity are criminal.

Date 1999-02-19 **Keyword** study survey insider crime sabotage industrial espionage computer crime

Source, Vol, No. National Business Review (NZ)

Allan Watt, director of forensic operations for computer security specialists S P Bates & Associates of New Zealand, said that his studies strongly support the view that 80% of computer crime is perpetrated by insiders. He said that many executives dismiss the consequences of computer crime as malfunctions and warns that it is unwise to allow I.T. staff to investigate suspected crime without supervision by forensic experts outside the department. His research also supports the widespread opinion that 90% of detected computer crime is unreported because of fears of embarrassment.

Date 1999-02-22 **Keyword** criminal hacker penetrations attacks China crime intrusion

Source, Vol, No. Reuters

The Chinese Department of Public Security announced that it had solved 100 cases of criminal hacking in 1998 but estimated that this was only about 15% of the actual level of unauthorized system access. Reported computer crime was growing at an annual rate of 30%, they said. About 95% of all Chinese systems on the Internet had been attacked last year, with many banks and other financial institutions the target of Chinese and international criminals.

Date 1999-02-23 **Keyword** survey crime fraud insider criminal hacker infowar espionage

Source, Vol, No. Australian

The annual Australian Computer Crime and Security Survey, organized by the Victorian Computer Crime Investigation Squad and Deloitte Touche Tohmatsu, reported on computer crimes in 350 of the largest Australian companies. In brief, the salient results were that about one third of the respondents had suffered one or more attacks on their systems in 1998; of those, 80% had experienced insider attacks, 60% experienced outsider attacks; and 15% of the respondents with any attacks claimed they had been the targets of industrial espionage. Almost three-quarters of all the respondents had no formal policy requiring notification of police authorities in case of attack. More than a fifth of all the respondents had experienced a breach of confidentiality and almost a fifth reported a breach of data integrity.

Date 1999-04-07 **Keyword** survey study computer crime costs defenses prevention

Source, Vol, No. Detroit News; < http://www.gocsi.com/prelea990301.htm >

The Fourth Annual Computer Security Institute / Federal Bureau of Investigation Computer Crime and Security Survey demonstrated yet again that computer crime is a growing problem for US companies, financial institutions and government agencies. Losses amounted to hundreds of millions of dollars, much of it resulting from industrial espionage. Key findings:
* 26 percent reported theft of proprietary information.
* System penetration by outsiders increased for the third year in a row; 30 percent of respondents reported intrusions.
* Those reporting their Internet connection as a frequent point of attack rose from 37 percent of respondents in 1996 to 57 percent in 1999.
* Unauthorized access by insiders rose for the third straight year; 55 percent reported incidents.
* More companies - 32 percent compared with 17 percent in the past three years - are reporting serious cyber crimes to law enforcement.

Date 1999-04-17 **Keyword** Internet crime detection enforcement international

Source, Vol, No. Reuters

Dick Satran summarized the computer crime scene for Reuters in mid-April. Computer crime is growing and international cooperation is insufficient to stop the perpetrators who take advantage of jurisdictional and technical problems on the law enforcement side.

Date 1999-04-19 **Keyword** computer crime criminal hacking penetration survey vulnerabilities firewalls

Source, Vol, No. OTC

M2 Communications reported in April 1999 that, a survey conducted for Infosecurity '99 and _Government Computing_ magazine found serious vulnerabilities among local authorities (municipal governments):
* 33% of local authorities in the UK were at risk of penetration by hackers
* 33% of local authorities lack firewall
* 6% do not have basic anti-virus software installed
* many of the systems with firewalls did not enable them to filter traffic.
A similar survey in 1998 suggested that 3/4 of medium-sized accountancy practices, law firms and PR and advertising agencies had no security measures in place at all.

Date 1999-04-20 **Keyword** survey management firewalls network viruses millennium

Source, Vol, No. InformationWeek UK via CMPWeb

Andrew Darling, writing for InformationWeek in the UK, penned a dismal litany of management failure to integrate security into their business operations. Interviews with many senior I.T. staff showed that the same decades-old pattern of ignoring security in favor of short-term focus on operations and profits makes it impossible for technical staff to do their job adequately.

Date 1999-04-30 **Keyword** survey e-mail servers vulnerability patch software

Source, Vol, No. OTC / PR

NTA Monitor Ltd released a survey of e-mail servers in British government systems showed that almost half had security vulnerabilities that made it possible for breaches of e-mail confidentiality. "The testing analysed the 689 Internet domains within the "gov.uk" name space, which includes central government departments, local government and a number of governmental organisations, and after discounting domains where no Internet email systems had been set-up, or which were not reachable during the tests, the survey reported on 345 live email servers." The analysis took place between November 1998 and April 1999.

Date 1999-05-03 **Keyword** criminal hacker damages loss theft controversy restitution

Source, Vol, No. LA Times <http://www.latimes.com/HOME/BUSINESS/CUTTING/t000039748.1.html>

The criminal-hacking magazine, _2600_, published letters from victims of Kevin Mitnick that estimated damages from his depredations. Total estimated costs (dismissed as preposterous by the _2600_ crew) were $292M, of which NEC claimed $1.8M and Nokia reported $135M.

Date 1999-05-13 **Keyword** privacy Web policies attestations assertions claims survey

Source, Vol, No. LA Times

A study by Georgetown University researchers revealed that about 66% of the 7,500 popular Web sites in the review included a privacy policy. Critics claimed that most of these were paying lip-service to privacy; Edupage editors wrote, "The FTC names five ingredients in its definition of a successful all-encompassing privacy policy, but [the] survey showed that just 10 percent of surveyed sites follow all five steps."

Date 1999-05-21 **Keyword** criminal hacking penetration vulnerability government report

Source, Vol, No. Reuters, AP

The General Accounting Office (GAO) of the US reported that some key computer systems at NASA are poorly protected against criminal hackers. "We successfully penetrated several mission-critical systems, including one responsible for calculating detailed positioning data for Earth-orbiting spacecraft and another that processes and distributes the scientific data received from these spacecraft. . . . [W]e could have disrupted NASA's ongoing command and control operations and stolen, modified or destroyed system software and data." Among other findings, the government auditors said that NASA failed to assess risks and evaluate security requirements; 135 of the 155 mission-critical systems reviewed failed the agency's own requirements for risk assessment. NASA provided inadequate computer security training, did not clearly classify information as public or confidential, and was unable to say how mission-critical systems should be protected from known threats from the Internet.

Date 1999-05-25 **Keyword** software piracy intellectual property theft copying

Source, Vol, No. Computer Reseller News Online

The Business Software Alliance and the Software and Information Industry Association announced a slight fall in piracy in 1998, although worldwide rates of unauthorized use remained at 38% (231M of a total of 615M new installations). Vietnam with 97% and China with 95% stolen software led the pack. Total theoretical losses were around $11B worldwide. However, the report also cited evidence that governments were working harder to reduce piracy.

Date 1999-05-27 **Keyword** survey study Internet usage children adolescents Web parental supervision involvement

Source, Vol, No. USA Today Online

A poll of 500 households showed that young people between 8 and 18 received minimal parental supervision in their use of the Internet. Some of the key points:
* 20% of parents did not monitor their children's Internet usage;
* 52% monitored usage only moderately;
* 18% of the children surveyed intended to physically meet someone they met on the Internet;
* 48% of parents allowed unlimited frequency of access to the Net;
* 24% of parents placed no restrictions on the length of time their children stay on the Internet;
* 71% of parents with children aged 14 years or older did not supervise their children's Internet use at all.

Date 1999-05-27 **Keyword** virus infection rates study survey

Source, Vol, No. Reuters

CERT-CC found that malicious software infections increased in the second quarter of 1999, with the Melissa and Chernobyl viruses causing widespread trouble.

Date 1999-06-16 **Keyword** criminal hacker attacks statistics study survey police business reporting intrusions

Source, Vol, No. Courier Mail (Brisbane, Australia), Sydney Morning Herald, Australian Financial Review

Studies by the Australian government contradicted accepted wisdom about the preponderance of inside attacks on business systems; the results suggested that most attacks were from outsiders rather than from disgruntled or dishonest employees. Apparently 42% of businesses said they did not report intrusions — implying that an astonishing (not to say unbelievable) proportion of 58% did report intrusions. Common agreement among security specialists has been that no more than 10% of all detected computer crimes are reported to authorities. Federal Justice Minister Amanda Vanstone everyone to stop seeing hackers "nerdy, pre-pubescent teens with youthful ideals." On the contrary, she said, "Increasingly, organisations around the world are experiencing attacks on their computer systems designed to financially benefit the perpetrator. This is a crime in the old-fashioned sense in that the motivation is greed."

Date 1999-06-18 **Keyword** economic impact costs expenses virus worm e-mail attachments damage harm consequences

Source, Vol, No. Computer Economics < http://mindfulness.com/new4/pr/pr990618.html >

A study by the Computer Economics firm estimated losses to victims of virus and worm infections at around $7.6B in the first half of 1999.

Date 1999-06-21 **Keyword** survey study consumer confidence suspicion worry e-commerce Web

Source, Vol, No. E-Commerce Times Online

In a study of 1,001 respondents selected at random among the general public, most people expressed suspicion about the security of online transactions. Highlights:
58% of consumers do not consider any financial transaction online to be safe;
67% are not confident conducting business with a company that can only be reached online;
77% think it is unsafe to provide a credit card number over the computer; and
87% want e-commerce transactions confirmed in writing.
The National Technology Readiness Survey was carried out by Rockbridge Associates over a two-year period.

Date 1999-07-12 **Keyword** virus hacker breaches survey attacks vulnerabilities

Source, Vol, No. InformationWeek < http://www.informationweek.com/shared/printArticle?article=infoweek/743/prs

A study of 2700 information technology professionals in 49 countries was summarized in July in InformationWeek. The Global Security Survey had many interesting findings; highlights:
* 64% of companies fell victim to a virus attack in the past 12 months, up from 53% the previous year
* In the U.S. alone, viruses hit 69% of companies, about four times as many as that of the next-highest category of security breach, unauthorized network entry
* 22% of companies reported no security breaches at all
* Hackers and terrorists were blamed for 48% of the security breaches, compared with 14% blaming hackers in 1998
* 31% of respondents blamed contract service providers for breaches (up from 9% last year)
* 41% blamed authorized users and employees (compared with 58% last year).

Date 1999-08-11 **Keyword** Internet hosts vulnerabilities scan report

Source, Vol, No. < http://www.securityfocus.com/templates/forum_message.html?forum=2&head=32&id=32%20%2

A small group of experts scanned 36 million Internet hosts in three weeks in December 1998. They published the results in August 1999. They tested for 18 vulnerabilities. They found 730,213 vulnerabilities on 450,000 hosts. They wrote, "These open points of penetration immediately threaten the security of their affiliated networks, putting many millions of systems in commercial, academic, government and military organizations at a high compromise risk."

Date 1999-09-01 **Keyword** online auctions fraud theft software copyright violations licenses

Source, Vol, No. IDG News Service

According to a study by the Software & Information Industry Association (SIIA), almost half the software sold online in auctions managed by eBay, ExciteAtHome and ZDNet violates the terms of the software licenses or is frankly pirated. Highlights of the findings covering 221 auction sales:
* 49% were illegal software
* 33% were legal
* 18% were of undetermined legality.
The 95% confidence limits for a percentages in a sample size of 221 are about ±8% for the 50% mark and decline steadily to about ±2% for lower values.

Date 1999-09-16 **Keyword** cyberwar information warfare infowar Trojan virus logic bomb back door criminal hacker penetra

Source, Vol, No. SANS, Computerworld Online

The SANS (System Administration, Networking, and Security) Institute warned in September that the Y2K gefuffle provides a perfect cover for disgruntled employees to install logic bombs and back doors. In addition, SANS experts warned that most computers have well-known vulnerabilities — Allan Paller estimates from 5 to 30 — that even novice criminal hackers can exploit.

Date 1999-09-22 **Keyword** software piracy theft Web fraud service support disappointment customer resentment

Source, Vol, No. USA Today

The BSA (Business Software Alliance) released a report showing that the number of Web sites peddling illegal copies of proprietary software grew from 100,000 in 1997 to 900,000 in 1999. Losses are estimated not only at around $11B but also in good will by customers innocently buying stolen software who are shocked (shocked!) at not receiving support from the publishers of the original software. [Hey wait a minute, what about all the people who buy legitimate copies of the software and are shocked (shocked!) at not receiving support from the publishers?]

Date 1999-10-03 **Keyword** study report vulnerability assessment infrastructure information warfare infowar

Source, Vol, No. Reuters

The General Accounting Office of the US government warned that the nation is increasingly vulnerable to information warfare and that the government is not doing enough to prevent damage. Areas of concern included air-traffic control, law enforcement, national defense and tax collection among others. As evidence of the rising threat, the GAO report cited statistics from the CERT-CC (Computer Emergency Response Team Coordination Center) at Carnegie-Mellon University, which handled 1,334 incidents in 1993; in the first half of 1999 the number was 4,398.

Date 1999-10-04 **Keyword** information warfare infowar Y2K threats attacks

Source, Vol, No. Reuters

By October, Worldwide preparations for Y2K-related disruptions were proceeding, with contingency plans for nuclear meltdowns, nuclear shutdowns, false alarms of missile attacks, and electronic attacks on critical infrastructure. In addition, many governments were concerned about disruption and violence from millennial cults and guerrillas looking for softened targets. Many jurisdictions have canceled police leave for the Y2K transition; some countries have canceled leave for the entire military.

Date 1999-10-05 **Keyword** survey information warfare Y2K vulnerabilities infrastructure trap doors logic bombs

Source, Vol, No. Newsbytes

The GAO issued a report, "Critical Infrastructure Protection: Comprehensive Strategy can Draw On Year 2000 Experiences," that emphasized the growing threat of information warfare. Sen. Robert Bennett (R-UT), chair of the Senate Special Committee on the Year 2000 Technology Problem, admitted that there might be a point to converting the Committee to a permanent group focusing on computer crime.

Date 1999-11-17 **Keyword** survey vulnerability networks outsourcing standards

Source, Vol, No. OTC

The Cutter Consortium reported that about 20% of 152 companies they studied had no information security standards at all. About 60% claimed they would implement such policies by the end of the year 2000. Only about 25% of the respondents said they had used security consulting companies for advice.

Date 1999-11-18 **Keyword** computer crime attacks vandalism penetration denial of service estimates survey conference

Source, Vol, No. TechWeb

Thomas Longstaff of the CERT-CC reported on the increasing number of cyberattacks, saying that the situation will only get worse as society increases its reliance on telecommunications for mobile computing and telecommuting. Speaking at the Annual CSI Conference in Washington, Dr Longstaff said that intrusion detection is a necessary component of today's security posture and added that computer emergency response teams are needed too.

Date 1999-11-29 **Keyword** fraud shopping e-commerce credit card debit

Source, Vol, No. Guardian

Gary Parkinson wrote an extensive review of e-commerce risks for The Guardian Weekly (1999-11-29, p. 13). Among his key findings:
* Some fraud artists trade legitimately online to establish credibility before exploiting online shoppers by withholding products or shipping shoddy substitutes or fake goods.
* Although most credit-card companies indemnify victims against losses, online users of debit cards are mostly out of luck if their money is stolen — debit card transactions are equivalent to cash purchases.
* "Visa says that half of all credit card disputes are about internet transactions, even though the net accounts for only 2 per cent of overall business. "

Date 1999-11-30 **Keyword** internal fraud statistics surveys studies report UK

Source, Vol, No. Corporate Insurance & Risk

Martin Allen-Smith wrote a summary of current studies on internal fraud in British corporations. According to his sources (quoting directly from his article),
* 75% of all companies have been hit by fraud at least once in the last five years. 41% have been hit five times or more.
* One in four UK companies have lost more than #600,000 in fraud in the last five years.
*Total UK company losses are estimated at 2% to 5% of annual turnover.
*Only 11% of corporate fraud losses are ever recovered.
*Fraud overtook bad debts as the major cause of business failure in the UK in 1996 according to The Society of Practitioners in Insolvency.
*More than 85% of UK companies believe that they are more at risk from fraud now than they were five years ago.
*The number of fraud charges made against companies by investors and investigated by the Serious Fraud Office has risen by 164% from 1993-96. In 10 of the 11 trials conducted in 1995, one or more of the company defendants were convicted.

Date 1999-12-06 **Keyword** survey e-commerce merchants ignorance liability fraud

Source, Vol, No. Newsbytes

The e-commerce firm CyberSource commissioned a survey of online merchants; the work was carried out by Mindwave and interviewed over 100 online businesses. The findings showed that 75% of the respondents rated credit-card fraud as "a concern" but only 59% knew that they would be liable for restitution in cases of fraud. About 72 percent of online merchants surveyed believed that sales would increase if online shoppers were not worried about fraud. The 95% confidence limits for percentages in a sample of 100 are approximately ±10% at worst.

Category 32 Censorship, indecency laws, 1st amendment (law)

Date 1999-01-01 **Keyword** children parents pornography Internet Web monitoring warning

Source, Vol, No. PA News

Peter Luff of the Conservative Party of Great Britain proposed a bill obliging computers to be sold with warning labels. Noxious emissions? Danger of shock? In a way: he wanted to be sure that parents were aware of the ease with which their children would be able to access pornography on the Net.

Date 1999-01-29 **Keyword** censorship Internet chat government fear persecution freedom

Source, Vol, No. AP, Washington Post

In yet another demonstration of the potential power of the Net, the Chinese dictatorship set up a 24-hour monitoring group to catch anyone making anti-government remarks. [Anything contradicting the Party line is defined as anti-government in China.]

Date 1999-01-30 **Keyword** child pornography digital editing law judgement court case

Source, Vol, No. AP, Washington Post

In Maine, a federal appeals court denied a defense against a child pornography conviction that was based on digital modification of innocent pictures of kids.

Date 1999-02-11 **Keyword** pornography First Amendment censorship university professors

Source, Vol, No. Washington Post

Six professors at Virginia universities protested the state law forbidding state employees from using employer-supplied computers to download pornography. They argued in court that their work on human sexuality and on sexually-explicit poetry was being hampered. The U.S. federal 4th Circuit Court of Appeals rejected their petition.

Date 1999-02-14 **Keyword** censorship China law repression Internet Web police ISP

Source, Vol, No. Australian AP

China's dictators established a taskforce in February to monitor Internet usage and to interfere with human-rights and pro-democracy groups' ability to use the network for anti-government activity. The ostensible reason for the draconian crackdown was the protection of state secrets; however, as Owen Brown of the Australian Associated Press reported, "in China even tomorrow's weather forecast is considered a national secret until its publication and release to the tightly controlled state-run media is approved by the relevant government authority."

Date 1999-02-15 **Keyword** Internet Web free speech censorship incitement violence law

Source, Vol, No. TIME Magazine

In Portland, OR in February, a jury handed down a $107M penalty against the anti-abortionists who, the plaintiffs argued, incited violence against purveyors of abortions. The "Nuremberg Files" Web site, complete with dripping-blood images, presented personal details about reproductive-center workers, including home address, the particular way they traveled to work, and even the names of their children. When "baby butchers" on the list were wounded, their names were changed to gray; when they were killed, their names were boldly crossed out.

Date 1999-02-19 **Keyword** child pornography Web Internet crime vigilante volunteer

Source, Vol, No. AsiaWeek

Toko's Metropolitan Police asked the Japanese chapter of the Guardian Angels to monitor the Japanese Internet for child pornography and other criminal activity.

Date 1999-03-19 **Keyword** pornography censorship government regulation ISPs Web

Source, Vol, No. Reuters

An Australian government bill would ban pornography and other objectionable materials on Web sites physically located in Australia and would also impose requirements on Australian ISPs to filter such materials. The international Internet Industry Association protested that such restrictions would be impracticable and argued for self-regulation and better tools parental supervision of Internet use by children.

Date 1999-04-08 **Keyword** information warfare hacking tools censorship culture subvert

Source, Vol, No. BORNEO BULLETIN

An article in the Borneo Bulletin reported on the growth of hacking in Brunei, where "officials, armed with red and black marker pens, painstakingly black out thousands of copies of undesirable pictures everyday, while undesirable computer software continue to flood the market."

Date 1999-04-19 **Keyword** free speech censorship Communications Decency Act lawsuit

Source, Vol, No. TechWeb, Reuters

In April, the SCOTUS upheld the part of the Communications Decency Act of 1996 which outlaws "the sending of any comment or image which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten or harass another person." This decision greatly offended the operators of <annoy.com>, a Web site that encourages anonymous e-mail to public officials. Lawyers for ApolloMedia argued unsuccessfully that some valid protected speech may offend some people but that constitutional rights to free speech should nonetheless apply.

Date 1999-04-20 **Keyword** library free speech censorship censorware evidence

Source, Vol, No. New York Times

David Butt, Librarian in Lake Oswego, OR launched a Freedom-of-Information campaign to collect factual information from libraries throughout the USA about the frequency of complaints about inappropriate use of library Internet-access computers. Butt, supported by the Center for Law and Policy at the American Family Association, a Christian group that backs censorship in Internet terminals in public libraries, is opposed to the position of the mainstream American Library Association, which argues that the problem is minor and that filtering software is inappropriate for institutions devoted to the dissemination of knowledge.

Date 1999-04-23 **Keyword** censorship legislation bill proposal

Source, Vol, No. <http://www.it.fairfax.com.au/breaking/924857680.html>

The Internet Industry Association of Australia rejected its government's proposals for Internet censorship. The Minister for Communications, Information Technology and the Arts had described legislation to force ISPs to conform to government instructions on blocking access to specific sites on the Web. ISPs protested that there are no foolproof steps to block such access and that the demand placed unreasonable demands on the entire industry.

Date 1999-05-11 **Keyword** censorship Internet Web content rating classification porn

Source, Vol, No. AAP

In Australia, a Senate committee approved The Broadcasting Services Amendment (Online Services) Bill 1999, which would extend the existing system of film classification to the Internet, outlawing RC and X rated material and making R material available only to people over 18 years. The bill remained to be approved by the entire Senate.

Date 1999-05-17 **Keyword** Canada Internet Web regulation content censorship law rules

Source, Vol, No. Wired

The Canadian Radio-television and Telecommunications Commission (CRTC) announced in May that it would not try to enforce requirements for Canadian content on the Net, arguing that most of the material is textual and therefore not covered by the Broadcast Act.

Date 1999-06-17 **Keyword** bill proposal law filtering obscenity child pornography library school constitution free speech cen

Source, Vol, No. C|Net

In June, the House of Representatives passed an amendment to the Juvenile Justice Bill (Bob Franks, R-NJ & Chip Pickering, R-MS) that would require schools and libraries receiving federal subsidies to impose filters on Net access to keep kids from viewing harmful materials.

Date 1999-09-01 **Keyword** government censorship law COPA Child Online Protection Act

Source, Vol, No. Wired via PointCast; EDUPAGE

The ACLU and other lobbyists for freedom of speech on the Net won an injunction against the Child Online Protection Act (COPA) passed in the closing days of 1998. US District Judge Lowell A. Reed Jr. ruled on 1 Feb 1999 that the law was too broad and must not be enforced. He also wrote in his memorandum that he considered the Act an unconstitutional violation of First Amendment rights of free speech: "Despite the Court's personal regret that this preliminary injunction will delay once again the careful protection of our children, I without hesitation acknowledge the duty imposed on the Court and the great good such duty serves. Indeed, perhaps we do the minors of this country harm if First Amendment protections, which they will with age inherit fully, are chipped away in the name of their protection." In September, COPA opponents including publishers, Internet companies, and trade associations filed an amicus brief in the Third Circuit Court of Appeals supporting the view that COPA was unconstitutional.

Date 1999-10-27 **Keyword** pornography censorship filtering academic universities state employees sexual content college A

Source, Vol, No. Washington Post

Half a dozen die-hard civil libertarians challenged the State of Virginia once again over its ban on state employees' accessing sexually-oriented materials from the Internet on computers in their places of work. The six professors, supported by the ACLU, argued that this law (ruled unconstitutional in early 1998 but reinstated in early 1999) violates the First Amendment. The State argues that because there is an exception for research approved by a professor's dean, the law is permissible.

Date 1999-10-29 **Keyword** Internet Web broadcasting authority government regulation control censorship pornography harm

Source, Vol, No. Australian Broadcasting Authority < http://www.aba.gov.au/about/public_relations/newrel_99/101n

The Deputy Chairman of the Australian Broadcasting Authority delivered a stirring call to government action on Internet regulation in the 1999 Spry Memorial Lecture in Vancouver, Canada. He called for national governments to exercise strict controls on Internet just as they control the airwaves for broadcasting. Oddly, he described the Net as "a means of mass communication of a particularly intrusive nature." He warned, "They [i.e., broadcast media and the Internet] enter our homes and workplaces, [and] exercise important influences on public life and national cultures. Their content has been and remains. . . of considerable concern to the public who wish to see national cultures preserved and enriched and to see young people protected from inappropriate material." He added later in his speech, "Whereas in the United States the US Constitution First Amendment allows the free speech lobby to dominate discussion about self-regulation, other countries with healthy democratic systems and vibrant processes of open expression are able to seek a more appropriate balance between the right to free expression and the right of communities to nurture national and local cultures and to protect children from harmful content."

Date 1999-11-30 **Keyword** censorship FBI police intimidation fraud lies

Source, Vol, No. <http://www.freedomforum.org/speech/1999/11/29closing.asp>

In mid-November, the president of an ISP in Michigan, BECamation, removed a satirical video from a user's Web site after FBI agents allegedly intimidated him by threatening legal action if he failed to act. In fact, the agents had no legal basis whatsoever for their demands. The video by New York artist Mike Zieper pretended to show an FBI training film discussing possible violence in Times Square because of putative Y2K problems. The FBI denied that any intimidation was involved.

Category 33 Acceptable-use policies, spam wars (corporate)

Date 1999-01-05 **Keyword** e-mail bombs flooding spam autoforwarding mail-storm

Source, Vol, No. PC Magazine <http://www.zdnet.com/pcmag/insites/dvorak_print/jd981208.htm>

Famed computer expert and commentator John C. Dvorak warned in one of his opinion columns in PC Magazine that feature-bloat in e-mail programs, trial accounts with ISPs and free e-mail providers were leading to uncontrollable spam and mail-bombing. For example, it was trivially easy to create a new free account, sign up for innumerable news lists with confirmation replies from that account, and then autoforward all the junk to an unsuspecting but soon-overwhelmed victim. Worse still, the victim would be unable to unsubscribe. Dvorak recommended a site for further information on the e-mail threat <http://www.silkroad.com/papers/html/bomb/>.

Date 1999-01-19 **Keyword** e-mail management policy attachment junk spam waste storm

Source, Vol, No. PC Magazine <http://www.zdnet.com/pcmag/insites/dvorak_print/jd981230.htm>

John C. Dvorak wrote in January 1999 that the lack of effective management policy on e-mail usage and storage is leading to a disaster for productivity. It's too easy to send e-mail; people store what they shouldn't; and people get involved in "mail storms" by forwarding message and appending the equivalent of "Me too" just to make their presence known. The author recommended strictly enforced guidelines for efficient use of this communications medium.

Date 1999-01-20 **Keyword** book spam instructions defense methods techniques

Source, Vol, No. RISKS 20 17

Alan Schwartz and Simson Garfinkel published _Stopping Spam_ in 1998 (O'Reilly, Sebastopol CA) ISBN 1-56592-388-X. The veteran and respected book reviewer Rob Slade, writing in RISKS 20.17, said, "All ISPs (Internet Service Providers), corporate network administrators, and net help desks should have a copy of this reference handy. Any serious Internet user will also find it well worth the price [U$19.95]."

Date 1999-02-17 **Keyword** telephone fraud abuse off-premises extension telco audit inappropriate use employees

Source, Vol, No. UPI

An article on the UPI news wire (author not listed) on 1999.02.17 noted that an audit of the District of Columbia showed that "more than one third of the 25,000 phone lines billed to the city are actually not being used for District business, costing the city $1.8 million a year." Inspector General E. Barrett Perryman is reported to have said that the "inspectors do not know how the lines ended up in non-city use."

[Comment from MK: Well, those of us who have been in the security field long enough know what's possible. A long-out-of-print book* on telephone fraud pointed out that it is ridiculously easy to generate "off-premises extensions" by fooling telco staff into adding additional numbers to a large account. When no one pays attention to exactly which lines are justified in the monthly bill, the extra lines can go unnoticed for months or years.]

* Haugh, J. J., R. E. Burney, G. L. Dean & L. H. Tisch (1992). _Toll Fraud and Telabuse: A Multibillion Dollar National Problem_. Telecommunications Advisors Inc (Portland, OR). ISBN 0-9632634-2-0. 399 + 431 pp.

Date 1999-02-17 **Keyword** pornography sexual harassment workplace civil liberties

Source, Vol, No. Atlanta Journal-Constitution

In Decatur, GA, three fire department supervisors were, um, fired when technicians found "inappropriate materials" (arson instructions? incendiary prose? hot porn?) on their computers. The department explained that city policies prohibit sexual harassment; however, the ACLU protested that "mere possession of sexually explicit material does not constitute sexual harassment" and said it might be a violation of free speech rights to prevent an employee from privately viewing such material during spare time on the job." [MK writes: From my point of view, it's the employer's equipment; if some owner wanted to prohibit viewing materials including the letter "e" using their computers, there would be no infringement of anyone's rights unless they were simultaneously ordered to accomplish useful work with those computers.]

Date 1999-02-25 **Keyword** spam legislation junk e-mail pornography government

Source, Vol, No. Washington Post, AP

In February, the Virginia legislature passed a law governing unsolicited commercial e-mail (spam). Spammers using forged headers to evade the consequences of their actions would be liable for conviction on a misdemeanor, with fines ranging up to $500. However, if a court decided that the spam was malicious and resulted in more than $2,500 in damages, the offense would become a felony with up to 5 years in prison. In addition, the legislation, which was signed immediately by Governor Jim Gilmore, allowed civil penalties of $10 per message to $25,000 per day. The ACLU vigorously opposed the legislation, arguing on constitutional grounds that it was an unwarranted intrusion on free speech. The ACLU was joined by the Gun Owners of America in its appeal to the governor of Virginia for a veto.

Date 1999-04-15 **Keyword** employee privacy e-mail monitoring confidentiality

Source, Vol, No. Wired, AMA <http://www.amanet.org/research/monit/index.htm>

The American Management Association surveyed 1,054 major US companies on their employee surveillance policies and found that 45% of the respondents monitor e-mail, phone calls and the content of computer files. About 84% of the firms inform their employees of this monitoring. See <http://www.amanet.org/research/monit/index.htm> for details

---

Date 1999-04-29 **Keyword** privacy e-mail corporate policy dishonesty evidence

Source, Vol, No. Guardian (London)

Michael Simmonds, head of marketing for the Tory party, leaked a document to the press using e-mail. A copy of the document was found in his electronic out-box and he was fired. Simon Waldman's _Guardian_ article warned that contrary to people's uninformed impressions, e-mail is far from transient; on the contrary, it has a permanence that can exceed that of paper documents. Backups, log files, reconstruction of erased files — any number of mechanisms can make e-mail available to the owners of corporate computer systems. If you don't feel comfortable making an e-mail communication available to your employer, don't write it on corporate computers. In addition, some people's marriages have been wrecked through indiscreet e-mail messages that later came to light; these documents have been introduced into court cases much to the embarrassment of the guilty mates.

Date 1999-06-14 **Keyword** spam survey study

Source, Vol, No. USA Today

GartnerGroup surveyed 13,000 e-mail users around the world about their experience with spam. The results were appalling:
* 90% of the respondents received at least one junk e-mail per week;
* 96% of those online for 4 years or more received junk e-mail at least once a week;
* 33% got 6-10 junk messages a week;
* ISPs lose ~7% of their new users every year because of disgust with spam;
* 40% of the respondents agreed that spam should be banned;
* 25% said that spam should be regulated;
* 25% despaired of solving the problem and simply deleted it;
* 3% of the respondents enjoyed it to some extent.

Date 1999-06-24 **Keyword** anti-spam automated Web site

Source, Vol, No. New York Times <http://www.nytimes.com/library/tech/99/06/circuits/articles/24spam.html>

Julian Haight detests junk e-mail, so he created a useful facility at <http://http://spamcop.net/> where anyone can submit junk e-mail for automatic followup. The free service parses the spam headers and sends polite e-mail to network administrators warning them about the junk e-mail originating from or being transmitted through their sites. For a modest fee, users can also sign up for an e-mail address that allows automatic filtering of spam and suspected spam, including various levels of severity such as automatic exclusion of e-mail from sites on a blacklist. The users of the free service indirectly help improve the paid service by allowing constant updates of the lists of known spammers. In addition, the site has a page of detailed statistics showing which ISPs and IP addresses are receiving the most e-mail from SpamCop concerning abuse.

Date 1999-10-13 **Keyword** spam junk unsolicited commercial e-mail law legislation bill proposal

Source, Vol, No. Newsbytes

The Unsolicited Electronic Mail Act was introduced to the House of Representatives by Heather Wilson (R-NM) and Gene Green (D-TX). This act would
* punish spammers with fines of $500 per message and $25,000 per day;
* define no-spam zones ("virtual gated communities") on the Net;
* allow individuals to post electronic "no trespassing / no spam" signs on their PCs and have mandated legal penalties for violation of those restrictions.

Date 1999-11-30 **Keyword** inappropriate use fired termination employee policy e-mail

Source, Vol, No. AP, Washington Post < http://www.washingtonpost.com/wp-srv/aponline/19991130/aponline1 930

More than 20 employees at the Norfolk, VA Shared Services Center of the New York Times were fired at once when management determined that they had sent "inappropriate and offensive" e-mail on company systems.

Date 1999-12-06 **Keyword** appropriate use policy termination e-mail

Source, Vol, No. Information Security Magazine Security Wire, Washington Post < http://www.washingtonpost.com/ 1 9

In late November, the New York Times Company fired 23 employees from its administrative services center in Virginia for violating its e-mail policies. No details were released other than to note that the problem involved inappropriate and offensive e-mail.

Category 34 Net filters, monitoring (technologies)

Date 1999-01-26 **Keyword** censorship filtering parental controls restrictions porn

Source, Vol, No. TechWeb

The RuleSpace Company announced a new pornography filter using the Intelligent Content Recognition Technology they claimed would make more reasonable distinctions about the content of sites using words such as "breast." The company said it opposed the use of filtering software in public schools and libraries and aimed its product at parents.

Date 1999-04-06 **Keyword** pornography cryptography encryption communications

Source, Vol, No. Business Wire

In an ugly development, pornography sites are providing strong encryption for their wares, making it difficult for investigators searching for evidence on data storage devices to accumulate evidence of illegal activity such as the use of child pornography. Encrypted porn is also impossible for filtering software to identify. The availability of NovaStor on the Web means that people can encrypt and decrypt files freely using the "Secret Service" function that simulates a safe using the company's DataSAFE software.

Date 1999-04-08 **Keyword** filter censorship restriction pornography lists keywords

Source, Vol, No. New York Times

Cybersitter and Clickchoice, makers of censorware, that favorite bugaboo of prepubescents everywhere, got into a legal battle over dirty words. Cybersitter accused Clickchoice of reverse engineering its proprietary list of filthy keywords and said it was considering a lawsuit. This situation may be fallout from the widespread cracking of censorware Naughty-Naughty lists; Cybersitter, in particular, was cracked in 1997 by Bennett Haselton, founder of the anti-censorware group Peacefire. The Index Verborum Prohibitorum was posted all over the Net within days, no doubt to the delight of the same prepubescents who didn't like the original product.

Date 1999-09-25 **Keyword** Web Internet ISP censorship rating pornography

Source, Vol, No. New York Times, Guardian (London)

The Internet Content Rating Association (ICRA) will try to create the first world standard based on RSACi, a rating system developed by the Recreational Software Advisory Council (www.rsac.org), a non-profit body in the United States. At a private meeting in Paris in mid-April, the major worldwide ISPs discussed how to help parents, schools and employers filter out objectionable materials more effectively than current methods. At present, the voluntary rating systems have managed to classify only about 1% of the world's sites; the new initiative would include better standards and more widespread publicity to encourage users to put pressure on providers to rate their sites. In addition, plans included spot checks to verify accuracy of the ratings.

Category 35 DNS conflicts, trademark violations (Net, Web)

Date 1999-01-05 **Keyword** DNS spoofing interception Web site e-mail vulnerability

Source, Vol, No. PR Newswire

Men & Mice, an Icelandic software developer <http://www.menandmice.com/>, warned of a serious vulnerability of many sites on the Internet. Using their DNS Expert analysis tool, they found that one-third of all the sites on the Internet were vulnerable to DNS spoofing. Using known vulnerabilities, criminals can send e-mail purporting to come from the victimized site, causing potential embarrassment and even legal liability in cases of mail-bombing attacks or widespread spam. Even worse, it would be possible to corrupt DNS tables to redirect connections to pirate sites; one scenario sketched out by the DNS expert Cricket Liu (of Acme Byte and Wire) ran as follows: "To picture the potential damage, envision visiting your bank's web site to transfer funds from one account to another. Unfortunately, the web site seems to be having problems: After entering your account information and PIN, you still can't access your account data. The web site reports a 'temporary failure' and invites you to try again later. What you don't realize is that the web site you see is actually a near-exact replica of your bank's web site -- startlingly easy to create -- and that you've just sent your account number and PIN to hackers in another part of the world. Though you entered the correct URL, your local name server had been spoofed into believing that the bank's domain name corresponded to the address of a web server run by hackers." On their own Web site, the company posted extensive information about how to combat DNS spoofing. Acme Byte and Wire also posted Cricket Liu's presentation, "Securing Your Name Server" at <http://www.acmebw.com/securing/index.htm>.

Date 1999-02-17 **Keyword** trademark infringement lawsuit lawyers attorneys Web sites DNS domain name system

Source, Vol, No. National Post (Canada)

The list of threats corporations attempting to defend what they see as their trademarks against Web sites using a variety of common names and words continued to grow in 1999. Simon Avery, writing in Canada's National Post, included the following cases:
* Playboy Enterprises Inc. and Estee Lauder Inc. sued Excite Inc. for infringing their trademarks in delivering URLs in response to searches by users.
* Archie Comic Book Publications threatened 23-month-old Veronica Sams because they claim that www.veronica.org violates their copyright on the name Veronica.
* Colgate-Palmolive sued the owners of Ajax.org because they were using the name of an ancient Greek hero — and scouring powder.
* Toys `R' Us sued Gus Lopez, owner of Toysrgus.
* Yahoo Inc. sued Yahooka, a guide to marijuana on the Internet.

Date 1999-02-17 **Keyword** trademark Web site copyright lawsuit DNS conflict squatters

Source, Vol, No. THE TIMES; Boston Globe

Jason Drummond, owner of VirtualInternet.net in England, helps companies protect themselves against cybersquatters who register domain names to take advantage of companies just getting started on the Net. Drummond was interviewed by John Kavanagh for The Times of London; he recommended that companies register as many variations on their trademarks as they can think of — with hyphens, underscores, abbreviations, acronyms, even likely misspellings. In another article, Jerry Ackerman wrote in the Boston Globe that some cybersquatters are getting rich on their claims; e.g., Compaq paid U$3.3M for the rights to <altavista.com>. Speculators also watch for mergers attentively. Ackerman wrote, "For example, six days before Exxon Corp. and Mobil Oil Corp. announced merger plans last Dec. 1, and continuing for a week afterward, five speculators - from Japan, South Korea, Singapore, Canada, and the United States - laid claim to 11 Internet addresses that joined the names of the two oil-industry giants."

Date 1999-02-23 **Keyword** cybersquatters DNS conflict trademark copyright domain name

Source, Vol, No. AP

In Houston, a federal court ruled in favor of Microsoft in a civil case against two cybersquatters who had registered eleven domains such as "microsoftwindows.com" and "microsoftoffice.com" as well as others such as "AirborneExpress.com", "AlamoRentaCar.com", "AssociatedPress.com" and "TravelersInsurance.com". Although the judge did not assign punitive damages, one of the defendants said through his lawyer that he was quitting the domain-name game.

Date 1999-03-10 **Keyword** DNS domain name system conflict adminstration

Source, Vol, No. Data Communications

In early March, the InterNIC of Network Solutions Inc. dropped thousands of entries from its domain name database, leaving those users bereft of their e-mail addresses and Web sites. Customers who were dropped were required to re-register for a fee. Some critics accused the firm of trying to get one last gasp of revenue before the ICANN (Internet Corporation for Assigned Names and Numbers) takes over in September 2000.

Date 1999-04-20 **Keyword** DNS domain name system allocation restriction licensing

Source, Vol, No. ZDNN

In April, Network Solutions Inc. lost its monopoly on domain name registration. ICANN, the Internet Corporation for Assigned Names and Numbers, announced five new registrars. The company agreed to make its database available to competitors. For a full of authorized registrars see <http://www.icann.org/registrars/accredited-list.html>.

Date 1999-04-22 **Keyword** Internet DNS domain name service fraud URL hijacking

Source, Vol, No. PR Newswire

Someone claiming to be a Portuguese resident called Carlos Pereira registered 25 domain names on the new .NU Domain Ltd domain name server in Britain. The perpetrator set up pornographic Web sites using .NU's quick-and-easy InstantWeb service and hijacked IP connections to legitimate Web sites. The .NU company revoked the perpetrator's accounts.

Date 1999-04-23 **Keyword** DNS domain name system ownership ISP conflict

Source, Vol, No. Network World Fusion <http://www.nwfusion.com/news/1999/0423domain.html>

One of the nastier side-effects of ICANN's monopoly busting decentralization of domain name registrations is that individual registrars could theoretically keep ownership of domain names they issue. Change registrar and you could find that someone else owns your trademarked domain. Such loss of control could be disastrous, forcing companies to change letterhead, business cards, and their entire Web sites. In addition, some ISPs are planning to offer domain-name services bundled into their contracts. Writing in Network World, Sandra Gittlen and Denise Pappalardo urged, "customers should check the fine print of their contracts to make sure that they retain rights to their online brands if they switch ISPs."

Date 1999-05-03 **Keyword** WIPO intellectual property DNS domain name squatters

Source, Vol, No. New York Times

In early May, the World Intellectual Property Organization (WIPO) of the United Nations proposed to ICANN (the Internet Corporation for Assigned Names and Numbers) that cybersquatting be outlawed. ICANN began evaluating the recommendations at a meeting in Berlin at the end of May.

Date 1999-05-05 **Keyword** DNS antitrust privacy database competition

Source, Vol, No. Washington Post

The DoJ began investigating the behavior of Network Solutions, Inc. (NSI), the firm which used to have a monopoly on Internet domain name registrations. The company refused to release their database of existing domains despite pressure from the National Science Foundation, which originally funded the company's operations. NSI also claimed that releasing its database might open the floodgates to junk e-mailers.

Date 1999-05-10 **Keyword** e-commerce Web Internet libel slander abuse complaints

Source, Vol, No. The Times (London)

Ian Brodie wrote an interesting article in _The Times_ (London, UK) summarizing some of the problems irritated consumers are causing businesses by creating critical Web sites that attract other people who are, depending on your perspective, angry victims of corporate greed or whining sore-heads who need to get a life. The canonical names for such sites include $1_sucks.com or $1_stinks.com, where $1 is the string variable representing some recognizable version of the exploiter/victim company. Some of the companies have responded with lawsuits; others with attempts to buy the offending DNS registration; and a few with cooperation and attention.

Date 1999-05-24 **Keyword** cybersquatters domain name registration DNS

Source, Vol, No. LA Times

A computer club in London, Pictureweb, managed to register 75,000 domain names between February and May 1999 through the ICANN-approved company "Register.com". Some of the club members registered thousands of names.

Date 1999-06-28 **Keyword** DNS domain name system registration conflict policy charges fees

Source, Vol, No. New York Times

In June, ICANN was forbidden by the US government to open its planned registration of Internet domain names to competition as several factions squabbled for control and oversight of the process. Critics didn't like ICANN's threat to cut Network Solutions Inc. (NSI) out of the registration business — especially since ICANN had no right to any such decision (it resides with the Dept of Commerce). Others questioned the new organization's right to levy a $1 annual fee on every registered domain.

In July, the test period for other companies offering to provide registration services was extended yet again, this time until 6 Aug 1999.

Date 1999-07-16 **Keyword** criminal hacker DNS domain name system

Source, Vol, No. Communications Week International

On 1999-07-01, criminal hackers hijacked Network Solutions Inc.'s Web sites (<networksolutions.com>, <netsol.com> and <thedotcompeople.com>) and rerouted would-be visitors to the CORE (Council of Internet Registrars) Web site — a competing domain-name system registrar. According to David Hotzman, NSI's CTO (Chief Technology Officer), someone made unauthorized template modifications of a host that changed the IP addresses of the NSI domain names. According to an article in _Communications Week International_, "The hack itself was a DNS modification spoof, whereby a person makes a modification to a domain name using NSI's public template interface, yet inserts data for a domain name owned by another party. NSI declined to comment on whether this was the first known attack of its kind, but said it has redesigned the system to protect against similar intrusions in the future."

Date 1999-07-20 **Keyword** pornography DNS domain name system registration obscenity

Source, Vol, No. Washington Post

Network Solutions Inc decided that other registrars would not be limited by the FCC list of seven forbidden words (yes, you know what they are) in domain name registrations.

Date 1999-07-30 **Keyword** cybersquatting DNS domain name registration trademark infringement law legislation bill propos

Source, Vol, No. Wall Street Journal < http://interactive.wsj.com/articles/SB933300984173737383.htm >

Orrin Hatch (R-UT) and others proposed a law to prevent people from using trademarked names belonging to others when establishing domain names for use on the Net. The bill provided for statutory damages and the right to appeal to the courts for seizure of the offending domain name.

Date 1999-10-05 **Keyword** DNS ICANN domain name system Web

Source, Vol, No. TBTF < http://tbtf.com/archive/1999-10-05.html >

ICANN, NSI and the Department of Commerce came to agreement in October over many elements of the new regime for naming Internet domains. According to Keith Dawson, editor of the always-useful TBTF newsletter (see < http://tbtf.com/archive/1999-10-05.html >), the key issues were as follows (direct quote from TBTF):
- NSI assents to ICANN's authority and agrees to sign a modified Registrar Agreement.
- Commerce takes over operation of the InterNIC.
- The fee NSI charges to competitive registrars drops from $9 to $6.
- NSI agrees in principle to a per-name fee to fund ICANN's operations, provided that NSI does not owe more than $2M under such a program. NSI hands over $1.5M to ICANN immediately.
- NSI continues to run the authoritative root server for at least four years. Even after its eventual transfer to ICANN, Commerce continues to assert policy authority to direct this server. [MK: I wonder what the EU thinks of this provision.]
- NSI must totally separate its registry and registrar functions-. If it accomplishes this within 18 months then it can hold onto the root server for an additional four years.
- NSI effectively gives up the claim that it owns the intellectual property represented by the .com/.org/.net database.

Date 1999-10-13 **Keyword** trademark infringement translation multilingual DNS domain name lawsuit

Source, Vol, No. Wired via PointCast News

Lawyers for WhatsHappenin.com sued quepasa.com for trademark infringement, claiming that the Spanish words were unacceptable because they constituted infringement, unfair competition and false advertising. Observers were watching the case with interest because its outcome could affect many sites whose names have the same meaning in various languages.

Date 1999-10-26 **Keyword** DNS hijacking search engines pornography criminal hacker

Source, Vol, No. Computer Currents 17 i20

Web hijacking can occur by copying legitimate Web sites, indexing them with search engines, then redirecting browsers to alternate — often pornographic — pages. The perpetrator can charge advertisers for all the unwilling hits on their sites. One villain who was shut down by the FTC even ran Java applets that disabled the "back" arrow in browsers and deleted the ability to close the browsers. People trapped in porno-hell had to reboot their computers to get out. Experts recommend that everyone keep an eye on the actual URL that appears in their browser window; any discrepancy between the visible URL and the actual URL should alert one to the possibility of fraud. In addition, consider running a personal firewall to block Java applets from unknown or untrustworthy sites.

Category 36 Responses to intrusion

Date 1999-01-12 **Keyword** information warfare criminal hackers retaliation attack

Source, Vol, No. CNN <http://cnn.com/TECH/computing/9901/12/cybervigilantes.idg/index.html>

When "The Electronic Disturbance Theater" criminal hackers attacked Pentagon systems in September 1998, the Pentagon retaliated by flooding the attackers with high-volume traffic, crashing the attacking systems. According to Winn Schwartau, some corporate security operations are taking the law into their own hands; he claims that one group actually located the headquarters of an attacking hacker group, broke into their facility, and stole the cybervandals' equipment. The corporate vigilantes apparently left a note saying, "See how it feels?" The same group also claims to have resorted to baseball bats to intimidate hackers.

Date 1999-04-17 **Keyword** information warfare defense retaliation intrusion detection

Source, Vol, No. OTC

Network Flight Recorder announced retaliatory software that not only detects and blocks the notorious Back Orifice program but also sends back misleading responses to attackers using the program

---

Date 1999-04-20 **Keyword** spam legal civil litigation settlement prevention damages

Source, Vol, No. TechWeb, ZDNet

Virgin Net, a UK Internet Service Provider, sued Adrian Paris, an alleged spammer whom they accused of sending 250,000 junk e-mail messages from one of their accounts in violation of their terms of service. In addition, the ISP was blacklisted by the Realtime Blackhole List, which provides participating ISPs with "kill lists" to block further e-mail from sites originating spam. The ISP received 1,500 complaints as a result of the abuse and sued the scumbag filthy disgusting spammer for breach of contract.

In a similar case, another UK ISP, Bibliotech, sued Sam Khuri and his Atlanta-based company, Benchmark Print Supply, after the American slimeball sent out junk e-mail with forged headers pointing to the innocent ISP; as a result, the enraged staff at Bibliotech were subjected to a "torrent of rejected, unsolicited commercial e-mail." In addition to damages, Bibliotech demanded that Khuri and his co-conspirators refrain from repeating their stupid trick with anyone else. In the USA, forged e-mail headers are currently illegal in Washington, Massachusetts and Virginia.

Category 37 Education in security & ethics

Date 1999-05-12 **Keyword** education universities learning research teaching NSA

Source, Vol, No. EE Times Online

In May, the National Security Agency named seven universities as Centers of Academic Excellence in Information Assurance Education: James Madison, George Mason, Idaho State, Iowa State, Purdue, Idaho, and the University of California at Davis.

Date 1999-08-01 **Keyword** criminal hackers sociology psychology harm morality ethics reasoning

Source, Vol, No. PC Magazine

John Dvorak wrote a blistering challenge to the nonsense spouted by criminal hackers when he wrote his column in PC Magazine on 2000-08-01. He provided a point-by-point rebuttal of the tired arguments of criminals that their depredations are actually socially useful. As Dvorak pointed out about the people who use Trojans to install back doors on victims' systems, "There's nothing good or noble about these Trojan horses or the people who use them. Eventually people will get on the systems of individual users, hack their online banking, and transfer money to themselves. Make no mistake about it, what appear to be harmless pranks today will be serious crimes tomorrow. As more and more people are adversely affected by these guys, the sympathy for them will fade to oblivion. The sooner the better." Dvorak's column made an excellent addition to the reading list for computer-ethics courses aimed at young people (and a slap in the face to the older fools who support criminal hacking).

Date 1999-10-01 **Keyword** education children school ethics anti-hacker surf law-abiding

Source, Vol, No. IDG.NET <http://www.idg.net/go.cgi?id=166554>

The Information Technology Association of America (ITA) announced a program of cooperation with the Department of Justice in educating children on ethical behavior in cyberspace. Many of the current criminal hacking incidents in recent years have involved juveniles, and other less criminal activities such as sending spam are "the modern-day equivalent of prank telephone calls" in the words of Keithe Perine, writing for <idg.net>.

Date 1999-10-18 **Keyword** information technology training basics CD-ROM DoD

Source, Vol, No. DoD DISA IPMO

At the 22nd NISSC in October 1999, the Defense Information Systems Agency INFOSEC Program Management Office (DIA IPMO) distributed free copies of a September 1998 CD-ROM entitled _Information Age Technology v 1.03_ which could serve as a good primer for novices about to take information security training in a corporate environment.

Other titles from the same source:

DoD INFOSEC Awareness v2.0 (April 1999)
Operational Information Systems Security Volumes 1 & 2 (August 1998)
CyberProtect Interative Training Exercise v1.0 (July 1999)
PKI — Public Key Infrastructure v1.0 (July 1999).

The same group distributed a May 1999 videotape containing four modules:
Computer Security 101 (DOJ)
Computer Security: The Executive Role (DOJ)
Safe Data: It's Your Job (DOL)
Think Before You Respond (NRO)

For information, send e-mail to <dodiaeta@ncr.disa.mil> or visit <www.disa.mil/infosec>. For an order form by fax, leave a message at 703-681-7944 or fax 703-681-1386.

Date 1999-11-18 **Keyword** criminal hacking juveniles international law enfocement investigation teaching video

Source, Vol, No. UPI

The FBI made an entertaining video about their capture of the kids involved in the February 1998 attack spree known as Solar Sunrise, where the Cloverdale Two hit DoD and other networks under the guidance of an Israeli criminal hacker, Ehud Tenebaum. The video was released in November with plans to make it widely available.

Category 42 Crypto algorithm weakness, brute-force attacks

Date 1999-01-20 **Keyword** cryptanalysis parallel processing crack DES challenge

Source, Vol, No. RISKS 20 17

The latest RSA challenge on cracking a message encrypted using the 56-bit DES algorithm was solved in about 22 hours by John Gilmore and the EFF's Deep Crack massively-parallel computing system and with the help of almost 100,000 volunteers around the world who attacked different parts of the keyspace. The EFF reported that the average search speed was 240 billion keys per second. Cryptographers agreed that the 56-bit DES is now inadequate as a method for securing data transmissions. The EFF won the grand prize of $10,000 for the feat.

Date 1999-02-15 **Keyword** PKI public key infrastructure dirty pair private criminal hackers

Source, Vol, No. INTERNETWEEK; Cylink <http://www.cylink.com/library/white/sterilize.htm>

According to scientists at Cylink, a network security vendor, it is possible for criminal hackers to develop "dirty" public/private key pairs to trick users of e-commerce. The scam would create keypairs that would allow different messages to have the same digital signature block; a criminal could thus spoof an authentic message by working backwards from the signature block, send the fraudulent message to the intended victim, and cause the public key cryptosystem to report a valid signature. The company recommended that proposed public keys be "sterilized" by a certification authority that would insert randomized data into the keys and provide mechanisms for legitimate users to modify their private keys accordingly.

Date 1999-08-15 **Keyword** encrypting file system cracked broken cryptanalysis algorithm bug defect debate disagreement an

Source, Vol, No. Crypto-gram 99 08

According to James J. Grace Senior and Thomas S. V. Bartlett III, Microsoft's Encrypting File System in Windows 2000 does not prevent discovery of disk decryption keys. A vigorous debate followed, in the "No it doesn't" — "Yes it does" style. See the story at < http://www.ntsecurity.net/forums/2cents/news.asp?IDF=118&TB=news >.

Date 1999-08-16 **Keyword** cryptography decryption TWINKLE engine brute force

Source, Vol, No. Wall Street Journal

Adi Shamir (the "S" in RSA) of the Weizmann Institute of Science in Rehovot, Israel announced a successful brute-force attack on a 512-bit RSA private key; the cryptanalysis took seven months and
required 292 computers at 11 different sites. However, Shamir also described the design for a $2M cryptanalytic computer called "TWINKLE" that could apply brute-force attacks successfully to RSA keys of 512 bits or lower keylength in a less than a week.

Date 1999-09-04 **Keyword** decryption brute-force parallel computing challenge supercomputer

Source, Vol, No. InformationWeek

The RSA-155 challenge (decrypting a message encrypted using a 155-bit RSA asymmetrical encryption private key) took six weeks of processing by a Cray 900-16 supercomputer, 300 SGI and Sun Microsystems workstations and Pentium PCs working in parallel. As the project director from the National Research Institute for Mathematics and Computer Science in the Netherlands, Herman Riele, said, ". . . Internet transactions protected by RSA-155 are still generally safe."

Date 1999-11-15 **Keyword** elliptic curve public-key cryptography cracked cryptanalysis parallel processing brute-force

Source, Vol, No. Crypto-gram <http://www.counterpane.com/crypto-gram-9911.html> 99 11

A group of cryptographers cracked a message encrypted with a 97-bit elliptic curve private key. The project required parallel processing by 740 computers and used 16,000 MIPS-years. Although Certicom, the company sponsoring the challenge, claimed that this result showed that the elliptic-curve algorithms are stronger than the RSA PKC, Bruce Schneier demurred, writing that the case was not yet proven. See < http://www.counterpane.com/crypto-gram-9911.html >.

Date 1999-12-04 **Keyword** encryption crack algorithm weakness DVD unlock movie

Source, Vol, No. Newsbytes

IBM, Intel, Matsushita Electric, and Toshiba, the member of the 4Cs industry group (the 4C Group soon became the 5C Group with the addition of Hitachi), chose a digital watermark standard for DVD-audio in June. However, in early November, the DVD Content Scrambling System (CSS) was cracked. The CSS was supposed to protect digital video disks against unauthorized duplication through a set of interlocking encryption keys and algorithms on the disks and in the players. The free DeCSS program, widely circulated on the Net, completely bypasses the encryption system. According to Mike Musgrove, writing for Newsbytes, "XingDVD Player, a program from Xing Technologies, a subsidiary of RealNetworks Inc., reportedly left this CSS software unscrambled--somewhat like leaving an extra set of car keys on the passenger seat. A small team of computer programmers in Norway used this vulnerability to design the DeCSS software. A spokesman for RealNetworks did not have a comment at press time."

In December, Matsushita Electric Industrial Co. and JVC announced a six-month delay in releasing their DVD-audio players because of concerns over protection of intellectual property. This was described in the press as the first case in which a cracked encryption scheme delayed a significant consumer-electronic product release. However, some sceptics noted that the music industry had already expressed reservations about supporting the CSS2 (the Content Scrambling System version used in protecting audio tracks), which was felt to be insecure.

[MK comments: This case demonstrates the foolishness of not posting cryptographic algorithms in public for strong analysis and testing. As Dorothy Denning said years ago , the security of an encryption algorithnm must not depend on its obscurity.]

Date 1999-12-06 **Keyword** cellular phone encryption algorithm cryptanalysis flaw bug weakness vulnerability

Source, Vol, No. Wired <http://wired.lycos.com/news/print/0,1294,32900,00.html>

Alex Biryukov and Adi Shamir of the Weizmann Institute in Israel published a paper showing how a simple PC was able to break the A5/1 encryption algorithm used in the GSM cryptosystem for cell phones in less than a second. Estimates were that more than 230 million cellular phones made by Ericsson, Motorola, Nokia, Siemens and other popular brands were vulnerable to such decryption. However, manufacturers pointed out that no one has ever demonstrated an ability to intercept a GSM phone call in real time, so the ability to decrypt the calls remains of academic interest. This assertion was challenged immediately by experts who pointed to easily-available, inexpensive scanner devices that successfully intercept GSM communications. Other spokespersons for the industry said that they would move to using published algorithms rather than relying on proprietary, secret algorithms for future encryption standards in the industry.

Category 43 New I&A products (tokens, biometrics, passwords)

Date 1999-01-01 **Keyword** forensic database ear prints criminals suspects evidence

Source, Vol, No. PA News

Scientists in Britain established the uniqueness of ear-cartilage patterns and successfully prosecuted a burglar who put his ear to a window to detect sounds in the home he burgled. The thief murdered a 94-year-old woman and was consequently sent to prison for life. The police authorities had gathered 1200 ear prints from volunteers by the end of 1998 and were hoping to begin collecting ear prints from suspects. The officer in charge of the project was John Kennerley, Chief Fingerprint Officer with Lancashire police; his work was based on pioneering research by Cor Van Der Lugt of the Netherlands.

Date 1999-07-01 **Keyword** biometric identification authentication I&A fingerprint scan banking financial transactions

Source, Vol, No. Future Banker

Randall Fowler, CEO of leading biometric authentication company Identix, said in a July article in _Future Banker_ that he thought banks would gradually introduce biometric I&A techniques such as fingerprint recognition to help secure financial transactions. For example, Motorola's new "Digital DNA" technology would allow fingerprint optics to be integrated into devices such as ATMs, phones and cash registers.

Date 1999-07-21 **Keyword** single sign-on identification authentication I&A passwords

Source, Vol, No. Computer Reseller News Online < http://www.crn.com/search/display.asp?ArticleID=7653 >

In July, Novell announced Single Sign-On 1.0, which supported multiple network logons with only one identification and authentication step for the user. The product was described as supporting Lotus Notes, PeopleSoft, Entrust and many other software systems.

Date 1999-10-12 **Keyword** medical informatics confidentiality HIPAA identification authentication I&A

Source, Vol, No. Wall Street Journal

Intel and the AMA announced that they would cooperate in implementing Internet Authentication Services for health-care workers exchanging confidential medical records.

Date 1999-11-15 **Keyword** biometric identification authentication I&A fingerprint bank Internet Web

Source, Vol, No. PRNewswire

SecuGen Corporation, SAFLINK Corporation, and ING Direct Canada announced plans for a fingerprint biometric security system for ING Direct's Internet banking products. Customers will use a finger-print recognizing computer mouse for identification and authentication.

Date 1999-11-17 **Keyword** biometric authentication signature face fingerprint

Source, Vol, No. Computer Reseller News

At the 1999 Fall Comdex, several companies introduced new or refined versions of their biometric authentication products. Bionetrix <http://www.bionetrix.com/> announced a new infrastructure for integrating a wide range of I&A products. Visionics <http://www.faceit.com/> continued to improve its facial recognition systems. CompuLink Research <http://www.clrusa.com/contactus.htm> announced its new U-Match fingerprint-reading mouse.

Category 44 New encryption algorithms, products

Date 1999-01-19 **Keyword** cryptography embedded encryption chip processor export

Source, Vol, No. Washington Post

Intel and RSA Data Security Inc. announced a plan to integrate RSA encryption into a new generation of processor chips. The companies envisaged improved security for e-commerce. Observers wondered whether the US government would stifle this effort by imposing export restrictions on the manufacturers.

Date 1999-01-28 **Keyword** laptop security smart cards inactivation theft encryption

Source, Vol, No. TechWeb

IBM announced that its new generation of ThinkPad computers would include automatic data encryption tied to the availability of a smart card. In addition, employers would be able to inactivate stolen computers as they leave the premises without authorization.

Date 1999-02-15 **Keyword** random number generator chip processor encryption algorithms

Source, Vol, No. Crypto-gram 99 02

Bruce Schneier, famed cryptographer and author of the Crypto-gram monthly free newsletter (see < http://www.counterpane.com for> details and back issues) hailed Intel's inclusion of a random-number generator on the new Pentium III chip. He wrote, "This is excellent news. I know nothing about how it works (or even if it is any good), but using techniques such as Yarrow, we can take even a mediocre hardware random number generator and turn it into something that is good for cryptographic applications." [Yarrow is Bruce Schneier and John Kelsey's pseudo-random number generator algorithm, available free from Counterpane Systems. See < http://www.counterpane.com/yarrow.html > for details.

Date 1999-02-23 **Keyword** hardware encryption anti-virus product access control

Source, Vol, No. PR

RVT Technologies, Inc. announced what they described as revolutionary PC-card based encryption, anti-virus and access-control technology for PCs.

Date 1999-03-15 **Keyword** encryption algorithm public-key cryptosystem cryptography portable hand-held

Source, Vol, No. Crypto-gram; PC Week < http://www.zdnet.com/pcweek/stories/jumps/0,4270,383613,00.html > 99 3

The Palm VII palm computer from 3-Com included elliptic curve public-key cryptography from Certicom.

Date 1999-04-14 **Keyword** encryption algorithm patent elliptic curve smart cards

Source, Vol, No. AMERICAN BANKER

RSA Data Security Inc. was awarded a US patent on "storage-efficient basis conversion," a technique that would enhance interoperability between different implementations of elliptic-curve cryptography. According to Jeffrey Kutler, writing in _American Banker_, "RSA said the existence of two common but conflicting numbering systems for ECC limits its usability and acceptance. Basis conversion is said to resolve the incompatibility between the polynomial and normal bases of calculation-and in a manner efficient enough to be handled within small or constrained computing appliances such as pagers, cell phones, or smart cards."

Date 1999-04-15 **Keyword** LINUX operating systems cryptography VPN virtual private

Source, Vol, No. Wired <http://www.wired.com/news/print_version/technology/story/19136.html?wnpg=all>

Linux aficionados gained a new tool for secure communications when the Linux Free S/Wan project released its new server software for virtual private networking over the Internet. Funded in part by the Electronic Frontier Foundation, the largely Canadian team of software engineers wrote the product despite resistance from elements in the law enforcement community who fear secure communications among criminals will make evidence-gathering much harder.

Date 1999-05-15 **Keyword** encryption algorithms tools kits

Source, Vol, No. Crypto-gram, < http://www.eskimo.com/~weidai/cryptlib.html > 99 05

Crypto++ v3.1 was released in May 1999. According to the notes on < http://www.eskimo.com/~weidai/cryptlib.html >, "Crypto++ is a free C++ class library of cryptographic schemes. Currently the library consists of the following, some of which is other people's code, repackaged into classes:
* a class hierarchy with an API defined by abstract base classes
* AES candidates: RC6, MARS, Rijndael, Twofish, Serpent
* other symmetric block ciphers: IDEA, DES, Triple DES, RC2, RC5, Blowfish, Diamond2, TEA, SAFER, 3-WAY, GOST, SHARK, CAST-128, Square
* generic cipher modes: CBC padded, CBC ciphertext stealing (CTS), CFB, OFB, counter mode
* stream ciphers: ARC4, SEAL, WAKE, Sapphire, BlumBlumShub
* public key cryptography: RSA, DSA, ElGamal, Nyberg-Rueppel (NR), BlumGoldwasser, Rabin, Rabin-Williams (RW), LUC, LUCELG, Elliptic Curve Cryptosystems
* padding schemes for public-key systems: PKCS#1 v2.0, OAEP, PSSR, IEEE P1363 EMSA2
* key agreement schemes: Diffie-Hellman (DH), Unified Diffie-Hellman (DH2), Menezes-Qu-Vanstone (MQV), LUCDIF
* one-way hash functions: SHA-1, MD2, MD5, HAVAL, RIPEMD-160, Tiger
* message authentication codes: MD5-MAC, HMAC, XOR-MAC, CBC-MAC, DMAC
* cipher constructions based on hash functions: Luby-Rackoff, MDC
* pseudo random number generators (PRNG): ANSI X9.17 appendix C, PGP's RandPool
* Shamir's secret sharing and Rabin's information dispersal scheme
* DEFLATE (gzip compatible) compression/decompression
* fast multi-precision integer operations
* prime number generation and verification
* various miscellaneous modules such as base 64 coding and 32-bit CRC
* A high level interface for most of the above, using a filter/pipeline metaphor
* benchmarks and validation testing.

Date 1999-08-16 **Keyword** Advanced Encryption Standard

Source, Vol, No. American Banker, Crypto-Gram 99 08

In August, the NIST announced the five candidates for the AES (Advanced Encryption Standard), the future replacement for the old 1976 DES. The minimum keylength of 128 bits should provide considerably greater security than the DES' 56 bits. Bruce Schneier published an excellent review of the situation in his Crypto-gram 99-08 < http://www.counterpane.com/crypto-gram-9908.html >.

Date 1999-09-28 **Keyword** encryption standard e-commerce wireless telephony public key infrastructure

Source, Vol, No. Financial Times (London)

Major telecomm players EDS (US), Ericsson (Sweden), Gemplus (France), & Sonera (Finland) formed the "Radicchio" forum to promote a global public key infrastructure that could support e-commerce through wireless devices such as mobile phones.

Date 1999-10-01 **Keyword** encryption e-mail Web startup new company service

Source, Vol, No. National Post (Canada)

Zero-Knowledge Systems of Montreal announced that three major venture capital companies had decided to invest in its Freedom 1.0 software project that will provide Internet users with strong encryption and privacy protection against tracking by Web site operators.

Date 1999-10-07 **Keyword** encryption confidentiality privacy e-mail temporary

Source, Vol, No. AP, USA Today

For those incapable of mastering PGP or other encryption programs, the Disappearing, Inc. company revealed its plans to make available encrypted e-mail with a sender-definable lifespan for the decryption keys kept on its servers. At the end of the lifespan, an encrypted e-mail message kept on its servers would no longer be readable. However, anyone who keeps a copy of the decrypted text of the self-destructing e-mail would be able to keep that indefinitely.

Date 1999-11-16 **Keyword** secure e-mail privacy self-destruct VPN server retract

Source, Vol, No. OTC

The 1on1mail.com company announced a new feature for its self-destructing secure e-mail. The server-based VPN e-mail allows cancellation of unread e-mail after it is sent. The PR materials issued by the company made some silly claims, though. Although the "Your Eyes Only" feature prevents Windows copy/paste operations, it may not defeat taking a snapshot using operating system features such as printscreen. The PR announcement also claimed, "1on1mail.com is also the only secure e-mail technology that keeps all messages encrypted in memory, not just to disk
like other e-mail solutions." [The notion that the information is kept encrypted in memory (with implication that it is not decrypted) is silly given that a readable version is on the screen. Where do these marketing droids think the screen version comes from? Mars?] This company also offered anyone capable of deciphering any of its encrypted e-mail "within a reasonable period of time" would be given $50K as a prize.

Date 1999-12-07 **Keyword** encryption 3DES European

Source, Vol, No. Reuters

Finnish telecommunication operator Sonera announced in December that it was the first non-US telecommunications firm to use the 168-bit 3DES algorithm in firewalls and virtual private networks (VPNs).

Date 1999-12-15 **Keyword** crypto algorithm fast matrices

Source, Vol, No. CNN news.com <http://www.news.com/News/Item/0,4,30930,00.html>

Sixteen year old genius Sarah Flannery of Cork in Eire invented a new approach to encryption that uses 2x2 matrices and looked to be even faster than the widely-used RSA algorithm for public key encryption. Cryptographers expressed interest but warned that it would be some years before the strength (resistance to cryptanalysis) of the new algorithm could be evaluated. In fact, however, Flannery herself cracked the algorithm and published the results in December 1999, eliciting praise from professional cryptographers.

Category 45 E-commerce security, digital signature, products

Date 1999-01-04 **Keyword** enterprise security data integration tool

Source, Vol, No. Business Wire

Internet Security Systems introduced SAFEsuite(R) Decisions to automate the collection, integration, analysis and reporting of enterprise-wide security information from multiple sources and locations including not only integrated data from ISS' intrusion and vulnerability detection systems, but also third-party security safeguards such as firewalls.

Date 1999-01-15 **Keyword** privacy government international standards business regulate

Source, Vol, No. Miami Herald

A working group of high-tech companies banded together in January to fight government regulation of Internet commerce. Founding members include America Online, Bertelsmann, Hewlett-Packard, IBM, MCI WorldCom, Netscape, Time-Warner and Vivendi.

Date 1999-02-03 **Keyword** e-commerce royalties intellectual property signature music SDMI Secure Digital Music Initiative

Source, Vol, No. Wired via PointCast

GoodNoise, a Web-based retailer of music, announced in February that it would henceforth brand all songs or albums downloaded from its site with a digital signature. In addition, the firm guaranteed that it would pay $0.07 per song for each download of a track through an agency to the copyright holder. The digital signature was not intended to prevent illegal copying but rather to provide a mechanism for honest purchasers to ascertain that they were acquiring a legally-copied and -distributed file.

Date 1999-02-17 **Keyword** digital watermark copyright copy protection

Source, Vol, No. New York Times

Hitachi, IBM, NEC, Pioneer and Sony (the "Galaxy Group") announced their agreement on a new digital watermark standard that would embed a cryptographic code in every frame of a digital multimedia work. New digital equipment would not allow copies of such works.

Date 1999-04-12 **Keyword** law legislation Congress digital commerce signature contract

Source, Vol, No. Internet World, Reuters

The Millennium Digital Commerce Act was introduced in the Congress of the US in April; the proposed law would define electronic contracts as legally binding instruments of trade. Sponsors include Sen. Spencer Abraham (R-MI) and John McCain (R-AZ), plus Rep. Anna Eshoo (D-CA). The ITAA expressed support for the legislation.

Date 1999-04-13 **Keyword** information warfare survey fraud theft gambling music piracy intellectual property law

Source, Vol, No. The Times of London

In Britain, pressure began to mount for government intervention in e-commerce. An article in _The Times of London_ reported, "The National Fraud Information Centre's list of leading Internet crimes includes web auctions (items bid for but never delivered); charges for services thought to be free; empty promises of business opportunities or franchises; false promises of credit cards to people with bad credit histories; and phony job agencies wanting fees to match people to jobs. Other cons range from bogus investments and false vacation offers to fake scholarship search services and fraudulent prize offers."

Date 1999-05-10 **Keyword** e-commerce Web credit card fraud heuristics AI detection

Source, Vol, No. Wall Street Journal

HNC Software Inc. announced extension of its credit-card monitoring services to Web merchants. Using neural nets for heuristic pattern-recognition of fraudulent transactions, the company has amassed a database of more than 260M credit card accounts' spending habits.

Date 1999-05-15 **Keyword** encryption trust management public key infrastructure PKI software tools

Source, Vol, No. Crypto-gram, < http://www.cis.upenn.edu/~angelos/keynote.html > 99 05

Matt Blaze, Joan Feigenbaum et al. released version 2 beta of KeyNote, a small toolkit for implementing trust relationships. The description at < http://www.cis.upenn.edu/~angelos/keynote.html > includes the following text from RFC 2704:
Trust management, introduced in the PolicyMaker system [BFL96], is a unified approach to specifying and interpreting security policies, credentials, and relationships; it allows direct authorization of security-critical actions. A trust-management system provides standard, general-purpose mechanisms for specifying application security policies and credentials. Trust-management credentials describe a specific delegation of trust and subsume the role of public key certificates; unlike traditional certificates, which bind keys to names, credentials can bind keys directly to the authorization to perform specific tasks.

Date 1999-05-15 **Keyword** smart card vulnerabilities common criteria protection profile credit-card

Source, Vol, No. Crypto-gram 99 05

According to Bruce Schneier, "Visa has issued a draft of the `Visa Smart Card Protection Profile,' as part of the Common Criteria. It contains a very nice list of smart card attacks. The document is a draft, and they want comments. < http://www.visa.com/nt/chip/accept.html http://jya.com/drpp-v.pdf >"

Date 1999-06-04 **Keyword** intellectual property watermark DVD audio copyright piracy

Source, Vol, No. TechWeb

IBM, Intel, Matsushita Electric, and Toshiba, the member of the 4Cs industry group, chose a digital watermark standard for DVD-audio in June.

Date 1999-06-14 **Keyword** online purchase buy e-commerce electronic wallet

Source, Vol, No. Wall Street Journal

Microsoft, Sun Microsystems, AOL, and IBM settled on a standard for establishing electronic wallets that would permit easy and safe electronic purchases by consumers. The ECML (electronic-commerce modeling language) would be supported by credit-card companies (VISA International and MasterCard International) and obviate the need for vendors to have special software. Consumers would be able to define their personal details and payment authorizations once on their own browsers and no longer have to re-enter these data for every electronic merchant.

Date 1999-07-19 **Keyword** digital signatures XML standard

Source, Vol, No. Network World Fusion< http://www.nwfusion.com/newsletters/sec/0719sec1.html >

In July, the IETF (Internet Engineering Task Force) and the W3C (World Wide Web Consortium) agreed on a plan to develop XML standards for digital signatures of documents on the Web. The working group aimed at establishing the new standards by the end of 1999.

Date 1999-08-05 **Keyword** e-commerce micropayments credit card phone company ISP Internet service provider

Source, Vol, No. Wall Street Journal

A number of companies appeared in 1999 to provide for micropayments online. These companies charge less than bank credit cards and share their revenues from retailers with the cooperating carriers. For example, iPin would allow consumers to add their tiny expenses online into a single payment through their local ISP. Similarly, eCharge would combine tiny charges into a single payment through a subscriber's phone bill.

Date 1999-09-29 **Keyword** secure PC encryption identification authentication access control smart card

Source, Vol, No. Business Wire

IBM announced its PC 300PL product line for secure electronic commerce. The secure desktop computers come equipped with an embedded security chip, smart-card access and data encryption.

Date 1999-10-12 **Keyword** privacy medical information identification authentication I&A doctors Internet remote telemedici

Source, Vol, No. Wall Street Journal

The American Medical Association (AMA) and Intel, the microcircuit manufacturer, combined forces to implement a public key infrastructure called "Internet Authentication Services" that would allow doctors to identify each other during the exchange of medical information over the Net.

Category 46 Cryptography exports from US

Date 1999-01-06 **Keyword** encryption Export Administration foreign programmers EAR

Source, Vol, No. CNET news.com <http://www.news.com/News/Item/Textonly/0,25,30590,00.html>

RSA Data Security Inc. (RSADSI), one of the leading US encryption firms, neatly evaded US export restrictions on strong encryption products by establishing an Australian subsidiary to sell encryption abroad. The U.S. Department of Commerce authorized the business as long as no U.S. employees or technology was used in the Australian business unit. However, there was some question about whether the Wassenaar agreement might impede RSA DSI Australia's success.

Date 1999-02-15 **Keyword** cryptographic export restrictions US government proposals

Source, Vol, No. Crypto-Gram; EPIC <http://www.epic.org/crypto/export_controls/bxa-regs-1298.html > 1999 02

On January 1, 1999, the Department of Commerce put into effect modified Export Administration Regulations with slightly more liberal allowance for commercial cryptography exports. The allowance for e-commerce involving banks was extended to merchants, insurance companies and medical applications. In addition, US corporations were permitted to use the same encryption tools for their foreign subsidiaries and some foreign partners.

Date 1999-02-26 **Keyword** encryption key escrow export committee law legislation proposal bill

Source, Vol, No. Benton; CyberTimes (New York Times), EPIC ALERT

Reps. Bob Goodlatte (R-VA), Zoe Lofgren (D-CA) and 205 other sponsors presented the Security and Freedom through Encryption Act (SAFE) for consideration by the Congress. The bill would eliminate restrictions on exports of encryption tools.

Date 1999-04-08 **Keyword** crypto export controls laws legislation bills

Source, Vol, No. NEWSBYTES NEWS NETWORK

Jim Lewis, the director of the Office of Strategic Trade in the Commerce Department's Bureau of Export Administration, predicted in April that "Any more major administration changes to US encryption export control policy are unlikely in 1999, along with any relaxation measures getting through Congress either." He was wrong.

Date 1999-04-09 **Keyword** encryption policy regulations restrictions law export

Source, Vol, No. CMP TechWeb

Shortly after warning that the Administration would NOT reconsider its export controls on encryption, Commerce Department official Jim Lewis, director of the Office of Strategic Trade at the Bureau of Export Administration, admitted that maybe it was time to change after all. According to a survey of 100 countries, "Only a handful of countries actually restrict encryption products," said David Banisar, policy director of EPIC, the Electronic Privacy Information Center. He was speaking at the 1999 Computers, Freedom, and Privacy Conference, a major annual meeting covering issues of privacy and technology. On 1999-4-19, John McCain and colleagues in the Senate of the US introduced a bill to liberalize cryptographic exports.

Date 1999-05-15 **Keyword** encryption exports restrictions teaching algorithms publishing free speech first amendment consti

Source, Vol, No. Crypto-gram, Wired 99 05

In 1997, Professor Dan Bernstein won a ruling that declared his Snuffle algorithm a form of speech and therefore not bound by the Export Administration Regulations. The government appealed the decision. In May 1999, the Ninth Circuit Federal Court of Appeals ruled in favor of the original ruling.

Date 1999-06-10 **Keyword** encryption exports restrictions foreign crypto products sales

Source, Vol, No. New York Times

A study by George Washington University computer scientists found that US restrictions on high-quality encryption software had not impeded the development and availability of strong cryptography in other countries.

Date 1999-06-24 **Keyword** encryption relaxation restriction bill legislation proposal law

Source, Vol, No. BENTON, Senate of the US < http://www.senate.gov/~commerce/press/106-82.htm >

In the US Senate, the Committee on Commerce, Science, and Transportation passed S.798, the PROTECT Act, a bill to promote electronic commerce. According to the press release (quoting directly), [t]he bill would do the following: 1) Direct the National Institute of Standards and Technology (NIST) to complete the establishment of an advanced encryption standard by January 1, 2002; 2) Allow for immediate exportation of encryption of key lengths of up to 64 bits; 3) Permit the exportation of non-defense encryption (above 64 bits) to responsible entities and governments of North Atlantic Treaty Organization (NATO), Association of Southeast Asian Nations (ASEAN), and Organization for Economic Cooperation and Development (OECD); 4) Allow for liberalization of export controls for encryption by creating an Encryption Export Advisory Board to review applications for exemption of encryption of over 64 bits and give recommendations to the Secretary of Commerce. The board would be made up of 12 members: the Under Secretary of Commerce for Export Administration, seven individuals appointed by the President (one from the National Security Agency, one from the Central Intelligence Agency, one from the Office of the President, and four representatives from the private sector who have experience in information technology), four representatives appointed by Congress (one by the Majority Leader of the Senate, one by the Minority Leader of the Senate, one by the Speaker of the House, and one by the Minority Leader of the House); 5) Give the Secretary of Commerce 15 days to respond to recommendations. If he rejects a recommended exemption, his decision is subject to judicial review; 6) Reaffirm presidential authority to veto a recommended exemption for national security purposes, and to establish terrorist and embargo controls; 7) Authorize increased funding to law enforcement and national security agencies to upgrade facilities and intelligence; and 8) Give the Secretary of Commerce the authority to prohibit the exportation of particular encryption products to an individual or organization in a foreign country identified by the Secretary.

The bill was then passed by the full Commerce Committee. According to the press release, there were several constraints on exports of encryption: "In approving the bill today, the Committee adopted --all by voice vote -- a number of amendments improving the bill. The Committee approved several amendments offered by Mr.Oxley (R-OH); one that allows the Secretary of Commerce to deny the export of encryption products to specific groups and organizations if it would be used to harm national security, used to sexually exploit children or used for illegal activities by organized; another amendment clarifies that despite a company's ability to export a product through encryption capabilities, the Secretary of Commerce may prohibit that product's export for other reasons; and a third amendment requires the Secretary of Commerce to consult with the Secretaries of State and Defense, Director of Central Intelligence and the Attorney General when conducting a technical review of an encryption product for export. The Committee also approved an amendment offered by Mr. Dingell (D-MI) that requires a comparable encryption product be available in a foreign country in order for a U.S. company to export similar encryption technology to that country. The Committee also approved two amendments offered by Mr. Stearns (R-FL); one that prohibits U.S. companies from exporting products to portions of China, specifically to the People's Liberation Army or the Communist China Military; the second amendment requires that if a person has been served a subpoena for access to encrypted information and if the person has the capability to decrypt the information but does not, then that person will be subject to additional criminal penalties."

Date 1999-07-14 **Keyword** encryption relaxation restriction bill legislation proposal law

Source, Vol, No. Newsbytes

The SAFE bill did not make it safely out of the clutches of the House International Relations Committee in mid-July. Opponents of relaxing encryption controls amended the bill with strict limitations at the behest of the FBI and the DEA. One amendment specifically prohibited all encryption exports to mainland China.

Date 1999-07-20 **Keyword** encryption relaxation restriction bill legislation proposal law

Source, Vol, No. POLITECH, ITI, Newsbytes

The President of the Information Technology Industry Council (ITI) urged the US House Armed Services Committee not to gut the SAFE bill. Another constituency supporting the SAFE Act was a group of former prosecuting attorneys in Congress. They wrote, "If US encryption continues to be restricted. . . foreign products will soon dominate the worldwide market, hindering our ability to gather intelligence against terrorists and criminals. . . . If cryptography can protect the trade secrets and proprietary information of businesses and thereby reduce economic espionage (which it can), it also supports in a most important manner the job of law enforcement. If cryptography can help protect nationally critical information systems and networks against unauthorized penetration (which it can), it also supports the national security of the United States." Despite the begging, though, the Committee did in fact ruin the bill from the point of view of its sponsors.

Date 1999-09-30 **Keyword** cryptography export controls key escrow search seizure fourth amendment constitution law propo

Source, Vol, No. USA Today; Crypto-gram 99 10

President Clinton issued a public letter on September 16th addressed to the Congress pushing for passage of the Cyberspace Electronic Security Act of 1999 (CESA), which simultaneously deregulates most encryption software exports and provides for key escrow accessible to law enforcement agencies under warrant.

Date 1999-11-24 **Keyword** encryption relaxation restriction bill legislation proposal law

Source, Vol, No. EDUPAGE, Washington Post

In September 1999, the Clinton Administration announced its intentions to liberalize encryption exports even further than the changes to the EAR that came into effect in January 1999. By late November, the Administration released another draft for comment, with final regulations due by December 15, 1999. The EDUPAGE editors summarized the situation as follows: "The proposed rules permit the export of retail encryption products with no restrictions on key length. In addition, the draft proposes looser export laws for open source software such as Linux. However, the rules might not apply to encryption software that is part of another program, and full bans would still exist for Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria. Some high-tech firms objected to the draft's unequal treatment of different types of encryption, saying tougher laws would apply to encryption that is built into hardware or software components."

Date 1999-11-24 **Keyword** cryptography regulations restrictions Department of Commerce limitations export license controls

Source, Vol, No. New York Times

In mid-November, the Clinton Administration began circulating its proposed new cryptographic export controls. However, according to critics and proponents of unregulated crypto exports, the actual proposals were far less liberal than original indications back in September. In particular, the export regulations continued to enforce license reviews for sales of cryptographic software and hardware to governments overseas.

Category 47 Key escrow / recovery laws

Date 1999-04-15 **Keyword** encryption legislation law proposal amendment key-escrow blocked debate

Source, Vol, No. Crypto-gram; ABC, Wired, CDT 99 04

In March 1999, a battle (but not the war) over key-escrow was won in the House Judiciary Committee. H.R. 850, the Security and Freedom through Encryption (SAFE) Act proposed by Rep. Lofgren (D-CA) was under attack by Rep. McCollum (R-FL), who proposed an amendment forcing mandatory key escrow as a condition for exporting encryption products. The amendment was blocked by Rep. Goodlatte (R-VA).

Date 1999-07-30 **Keyword** tax benefit encryption key escrow back door

Source, Vol, No. Wired < http://www.wired.com/news/print_version/politics/story/21014.html?wnpg=all >

In July, Reps. Porter Goss (R-FL) and Julian C. Dixon (D-CA) sponsored HR2616, another attempt to encourage key-escrow or law-enforcement-enabled cryptographic software. The bill would give a 15% tax reduction to firms on the costs of developing encryption software with easy access to government-authorized eavesdroppers.

Date 1999-08-20 **Keyword** privacy warrant decryption encryption law enforcement

Source, Vol, No. Washington Post < http://www.washingtonpost.com/wp-srv/business/daily/aug99/encryption20.htm

In August, the Department of Justice proposed the Cyberspace Electronic Security Act, which would allow law enforcement, under warrant, to install software that would disable encryption on personal computers in suspects' homes and offices. The Computer & Communications Industry Association (CCIA) joined with civil liberties organizations in immediately condemning the proposal as a covert intrusion into private homes and offices. [Seems to me that requiring a warrant for installation of the systems and requiring another warrant to read the data provides a pretty strong protection of the citizen. How is this process any weaker than getting a warrant to use binoculars in collecting evidence of wrong-doing?]

Date 1999-09-04 **Keyword** Windows software key NSA controversy overblown rumor jumping conclusions

Source, Vol, No. Various sources including Washington Post, , New York Times, NTBUGTRAQ. RISKS

Andrew Fernandes of Cryptonym, a Canadian security firm, seems to have gone off half-cocked when he found a signing key for integrating cryptographic modules into Windows that was labeled "NSA Key." He and other conspiracy buffs interpreted this label to mean that there was somehow a back door into Windows that would allow the National Security Agency to integrate its own cryptographic modules into the operating system yet have the version check out using digital signature verification. Such manipulations could generate versions of Windows with a back door for the NSA. Microsoft denied this interpretation (Aha! Told you!) and claimed that the key was "compliant with the NSA's technical standards." A particularly clear discussion by Russ Cooper <Russ.Cooper@RC.ON.CA> on NTBUGTRAQ pointed out that the conspiracy theory was farfetched but warned that it would be indeed be possible for anyone to insert their own cryptographic modules into Windows and sign them using their own digital key, thus allowing foreign cryptographic code to run under Windows even without signature by Microsoft or approval by the US Dept of Commerce under the Export Administration Regulations.

Category 48 Foreign crypto & computer crime laws (not cases or sentences)

Date 1999-01-13 **Keyword** criminal hacking intrusion penetration law jurisprudence

Source, Vol, No. <http://www.infobeat.com/stories/cgi/story.cgi?id=2558024618-6dd>

The Supreme Court of Norway ruled in January 1999 that attempted penetration of a network or computer system is not in itself a criminal act until it succeeds. Critics argued that such a position was, in the words of Doug Mellgren writing for Associated Press, analogous "to allowing a burglar to check all the doors and windows of a house for locks and not prosecuting them until they actually break in."

Date 1999-01-19 **Keyword** cryptography laws rules restrictions France government

Source, Vol, No. Crypto-gram; Slashdot < http://slashdot.org/articles/99/01/19/1255234.shtml > 99 02

In January, the French government relaxed its restrictions on commercial cryptography. The announcement ended the insistence on key escrow and allowed keylengths jumped to 128 bits for single-key encryption algorithms. The US reportedly tried to put pressure on the French through the Wassenaar Arrangement that tries to force strong export controls on encryption among all the signatories. As Bruce Schneier and many other critics of this policy have noted, "This only makes sense if the U.S. is the only source of strong cryptography. But it isn't — overseas security software is now just as good as work done by U.S. programmers. . . ."

Date 1999-01-20 **Keyword** censorship hacktivism espionage crackdown prosecution

Source, Vol, No. Washington Post

Chinese authorities imprisoned 30-year-old Lin Hai, a computer software entrepreneur, for having sold a list of 30,000 Chinese e-mail addresses to the dissident-supporting group VIP Reference of Washington DC. The sentence was for "only" two years -- significantly lighter than recent punishment for other dissidents.

Date 1999-02-15 **Keyword** Japan cybercrime penetration law

Source, Vol, No. ABIX - AUSTRALASIAN BUSINESS INTELLIGENCE

In Japan, rumors surfaced in 1999 that the Diet would draft laws making it illegal for criminal hackers to penetrate computer and network perimeters without permission. Current Japanese laws did not criminalize breaches of confidentiality, only breaches of integrity or of availability.

Date 1999-03-11 **Keyword** DNS domain name system WIPO law Internet

Source, Vol, No. RISKS 20 24

Prof. Michael Froomkin (U. Miami) published a blistering attack on the proposals for controlling the DNS (domain name system) put forth by the WIPO (World Intellectual Property Organization); see <http://www.law.miami.edu/~amf/quickguide.htm>. According to Froomkin, the main problems with the WIPO plan are as follows (numbering and some punctuation added):
"(1) Bias. The plan is biased in favor of trademark holders;
(2) Enabling censorship. The WIPO plan fails to protect fundamental free-speech interests including parody, and criticism of corporations;
(3) Zero Privacy. The WIPO plan provides zero privacy protections for the name, address and phone number of individual registrants;
(4) Intimidation. The WIPO plan creates an expensive loser-pays arbitration process with uncertain rules that will intimidate persons who have registered into surrendering valid registrations;
* Tilts the playing field. The WIPO plan would always allow challengers to domain names registrations to appeal to a court, but would often deny this privilege to the original registrant;
* Smorgasbord approach to law. Instead of directing arbitrators to apply applicable law, WIPO proposes using additional, different, rules it selected--rules that will often disadvantage registrants.

Date 1999-04-12 **Keyword** legislation laws proposals government criminal hacking computer viruses government

Source, Vol, No. NZ Press Assoc.

Justice Minister Tony Ryall of the New Zealand government announced in April 1999 that he would be proposing changes to the Crimes Act to define four new offences that harm computer users:
* accessing a computer system for a dishonest purpose,
* attempting to access a computer system for a dishonest purpose,
* damaging or interfering with a computer system and
* unauthorised access to a computer, commonly known as hacking or cracking.

Date 1999-04-13 **Keyword** Internet social policy dangers crime government culture

Source, Vol, No. THE DAILY STAR (Beirut, Lebanon)

The first pan-Arab conference on Internet security opened in Beirut in mid-April with speakers and participants from Lebanon, Saudi Arabia, Oman, Yemen, Bahrain, Jordan, Syria and Qatar. Speakers described the Internet as "an irreplaceable means of development" but also warned of the perceived perils of unfettered access to the Net. Author Alia Ibrahim, writing for the _Daily Star_ in Beirut, reported, "Saudi scientist Abdel-Rahman Abed Al-Wahed said that it was nonetheless a potentially dangerous technology that needed constant supervision."

Date 1999-04-17 **Keyword** criminal hackers punishment hanging death penalty execution

Source, Vol, No. National Post (Canada) <http://www.nationalpost.com/commentary.asp?f=990407/2456715>

A Montreal journalist apparently seriously proposed that criminal hackers should be hanged, just like coin clippers in Britain the 18th century or horse thieves in the USA in the 19th century. She argued that these activities all threaten the economic system in fundamental ways and that lenient treatment of the malefactors encourages copy-cat behavior. [MK comments that children and adolescents are among the criminal hackers who cause harm, but children and adolescents are notoriously poor at making rational judgements based on planning for consequences of their actions.]

Date 1999-06-10 **Keyword** encryption controls restrictions worldwide international study report

Source, Vol, No. EPIC Alert < http://www2.epic.org/reports/crypto1999.html > 6 09

The Electronic Privacy Information Center released its second annual survey of encryption restrictions around the world. The paper was available electronically at < http://www2.epic.org/reports/crypto1999.html >. In general, few countries restricted the use, manufacture or sale of encryption products. As yet another slap in the face of encryption-restriction supporters in the US, the report pointed out that at least 167 foreign cryptographic products use strong encryption in the form of these algorithms: Triple DES, IDEA, BLOWFISH, RC5, or CAST-128. The report also identified 512 foreign companies that either manufacture or distribute foreign cryptographic products in at least 67 countries outside the United States.

Date 1999-10-04 **Keyword** pedophiles criminal hackers United Kingdom England UK police law enforcement crackdown pr

Source, Vol, No. Reuters

In October, the British government announced a far-reaching plan to fight computer crime. "In order for the Internet to thrive it must be a safe place for business and leisure and protect the freedoms of internet users," said the Home Office Minister, Charles Clarke. Police would be working with the privately-funded Internet Watch Foundation, where monitors would alert them to illegal materials on the Web such as child pornography.

Date 1999-11-22 **Keyword** computer crime legislation punishment severity proposal resport government

Source, Vol, No. INFOTECH (NZ)

The New Zealand Law Commission recommended that the government define any unauthorized intrusion into a computer system or network as a computer crime. Six months before, they had hesitated and suggested that an intrusion would be a crime only if the prosecutor could prove malicious intent or actual damage. The May 1999 report said, "An intent to cause loss or harm, or an intent to gain a benefit or advantage is needed to avoid trivialising the criminal law by making every unauthorised access a criminal offence." The November version said, "We are now persuaded that that view was too narrow".

Category 49 Privacy, surveillance by law enforcement / govt, privacy legislation

Date 1999-01-02 **Keyword** police database personal information privacy Europe

Source, Vol, No. The Times (London)

The Europol Computer System (TECS) began operations in 1999, causing widespread alarm among privacy advocates (and, one hopes, criminals as well). The database, established to support crime-fighting by the new 15-nation police intelligence agency for the European Economic Union, stores not only information about criminals but also about suspects, victims and even potential victims. By law, the data should be available only to authorized law enforcement officers; however, a recent case in which a Belgian policeman passed data from another police database to the Mafia has caused alarm among civil rights activists.

Date 1999-01-06 **Keyword** lawsuit ISP privacy database personal information data

Source, Vol, No. Wired <http://www.wired.com/news/print_version/email/member/politics/story/17188.html>

The Aware Woman Center for Choice in West Palm Beach, FL sued CompuServe in January for allowing abortion foes to collect enough personal information to support terrorism against abortion supporters. Abortion foes recorded car license plates of visitors to abortion centers and then used NY-based TML Information Services' databases to look up the home addresses of the car owners. TML makes its services available for a fee through CompuServe and other ISPs.

Date 1999-01-07 **Keyword** espionage privacy international surveillance communications

Source, Vol, No. Daily Telegraph, Guardian

Privacy advocates blew a gasket when Enfopol 98 was revealed -- a Europe-wide system for monitoring telecommunications for police purposes. All European ISPs and telcos would be required to provide real-time, full-time access to all electronic communications regardless of where the calls originate. Even satellite-based systems such as Iridium would have to comply with these requirements. Enfopol would tie in with FBI plans as well for global electronic surveillance. After the revelation by the German Internet magazine _Telepolis_, the fate of the legislative proposals was in doubt. In early April, the Members of the European Parliament decisively rejected the proposal.

Date 1999-01-12 **Keyword** digitised signature driver's license

Source, Vol, No. THE DOMINION (New Zealand)

The New Zealand government announced that new driver's licenses would bear a digitised signature. An opposition member of the legislature, Neal King, protested that storing such signatures in insecure databases would lead to disaster.

Date 1999-01-19 **Keyword** privacy homosexual military navy AOL ISP

Source, Vol, No. CyberTimes via Benton Project; New York Times <http://www.nytimes.com/library/tech/99/01/cyb

In January 1999, Tim McVeigh was honored by _Out Magazine_. The Navy veteran was thrown out of the military when someone reported that his AOL account showed marital status "gay." With the help of the Electronic Privacy Information Center (EPIC <http://www.epic.org>) and of the Servicemembers Legal Defense Network <http://www.sldn.org/>, he won legal battles to be re-admitted to the Navy. Unfortunately, he was not returned to an equivalent job.

Date 1999-01-20 **Keyword** privacy database sex offender individual rights errors data

Source, Vol, No. RISKS 20 17

The Virginia state database listing known sex offenders -- and their addresses -- quickly ran into trouble. In the first three weeks, 49 residents of the state were listed in a weekly publication as sex offenders; two of those addresses were wrong. The ACLU very properly said I-told-you-so.

Date 1999-01-22 **Keyword** privacy chip serial identifier processor e-commerce

Source, Vol, No. Washington Post, San Jose Mercury News, New York Times, AP, New York Times < http://www.ny 20 19

A storm of protest erupted when Intel innocently announced what it thought would be a useful feature: software-accessible microprocessor serial numbers. Apparently unaware that minicomputer and mainframe manufacturers have provided such a feature for decades, privacy activists — including in particular the Electronic Privacy Information Center <http://www.epic.org> — appealed to the FCC to stop what they perceived as a nefarious plan to invade consumer's privacy. Intel's Pentium III chip includes a software-accessible serial number, just like LAN interface cards and many other kinds of processors long used in industry. Civil libertarians protested that such a unique identifier would allow detailed tracking of an individual's usage of the Internet. Bowing to protests, the company later agreed to set the default for this feature to "off." Critics than insisted that the mere availability of the feature would put pressure on consumers to turn it on; as Deirdre Mulligan of the Center for Democracy and Technology said, "If everybody's demanding it, it's going to be hard for a consumer to say no." Later in February, Junkbusters Corp. and EPIC (Electronic Privacy Information Center) appealed to the Federal Trade Commission for a ruling forbidding the chip from being released. The FTC declined to cooperate. The situation was inflamed by the discovery in late February that the software switch could be activated remotely, without permission of the PC owner. In late February, a German magazine, Computer Technology, published reports that the feature could be hacked to change the unique identifier, thus allowing a breach of authenticity by altered computers. Pentium determined that the problem lay in the software it had released.

Date 1999-02-08 **Keyword** privacy software Web Internet pseudonyms concealment

Source, Vol, No. LA Times

Zero Knowledge Systems announced its new Internet privacy software product, appropriately called "Freedom." This package, available in March, would provide for multiple pseudonyms, controls cookies, and spam filters.

Date 1999-03-03 **Keyword** privacy wireless communications eavesdropping law

Source, Vol, No. tele.com

In late February, the US Congress passed The Wireless Privacy Enhancement Act. This bill criminalizes eavesdropping on any form of wireless communications (analog or digital) and sets fines and possible imprisonment for violations. The act would also require the FCC to ban scanners capable of eavesdropping on such communications.

Date 1999-03-08 **Keyword** serial number Windows operating system unique identifier privacy protests

Source, Vol, No. BENTON Project; Washington Post

Microsoft announced that it would distribute a program to eliminate the unique processor-ID that Windows 98 stamps on every document created under that version of the operating system. Privacy advocates had been up in arms about the number, which was in fact used in 1999 to track a malefactor, David L. Smith, author of the Melissa e-mail enabled worm.

Date 1999-03-08 **Keyword** privacy confidentiality signature imprint serial number

Source, Vol, No. AP

A Brookline, MA programmer caused a furore when he discovered that Microsoft's Windows 98 operating environment attaches a unique system-identifier to every document produced on a PC. Microsoft responded quickly by providing a patch to turn off this "feature." See < http://officeupdate.microsoft.com/Articles/privacy.htm >.

Date 1999-04-04 **Keyword** information warfare privacy virus serial number stamp Word

Source, Vol, No. THE NEW YORK TIMES NEWS SERVICE

As the search for the author of Melissa, generally accepted to be someone calling himself "Vicodin ES," continued, investigators discovered a serial number in the vector document, written with MS-Word. The undocumented serial number not only helped law enforcement catch the perpetrator (30-year-old programmer David L. Smith of Aberdeen, NJ) it also caused a fuss among privacy activists world wide. Amitai Etzioni, a professor at George Washington University and author of _Limits of Privacy_, said, "The No. 1 threat today to privacy is not Big Brother, it's big bucks."

Date 1999-04-08 **Keyword** privacy legislation bill proposal US law regulation

Source, Vol, No. PC WORLD DAILY

In April, Congressional Rep. Ed Markey (D—MA) announced his bill to establish a national privacy policy, bringing the US up at last with nations around the world who established such policies — and Privacy Commissioners or Privacy Ombudsmen — years ago. Writing in _PC WORLD DAILY_, Niala Boodhoo summarized the issues as follows: "The proposed policy boils down to three basic principles: the individual's right to know what personal information is being gathered; the right to know whether gathered information may be used for other purposes; and the right to refuse to provide information."

Date 1999-04-15 **Keyword** anonymity anonymizer vulnerability hacks weaknesses quality assurance

Source, Vol, No. New York Times

Richard M. Smith, President of Phar Lap Software of Cambridge, MA reported on weaknesses in anonymizer products promising users protection against disclosure of their identity. Peter Lewis wrote in the _New York Times_, "Anonymizer.com (www.anonymizer.com), the Naval Research Laboratory's Onion Router (www.onion-router.net), the Lucent Personalized Web Assistant service (www.bell-labs.com/project/lpwa) and . . . Aixs.Net (aixs.net) were scrambling this week to patch the security holes."

Date 1999-04-16 **Keyword** privacy browser bookmark Web

Source, Vol, No. Wired

Kevin Cooke, Development Manager at Wired Magazine, discovered that Microsoft's Internet Explorer version 5.0 sends information to a Web site when the user bookmarks the site's URL. Chris Oakes of Wired reported: "This is one of those things where we did not see the privacy issue when we were creating the feature," said Microsoft product manager Mike Nichols. "The feature doesn't pose a super-huge risk. But Microsoft is looking at ways of modifying this feature in future releases." Apparently the feature was designed to allow a Web site to supply an icon to be stored on the user's system so any "Favorite" would be "branded" with that icon.

Date 1999-04-16 **Keyword** privacy policy Web federal government agencies browsers

Source, Vol, No. Wired

The Center for Democracy and Technology published a study in April showing that only about a third of US Federal Government agencies actually publish detailed privacy policies showing visitors exactly what kind of data their Web sites collect.

Date 1999-04-20 **Keyword** bank secrecy reporting privacy customer data police law

Source, Vol, No. AP

Congressman Ron Paul, (R-TX) proposed repeal of the 1974 Bank Secrecy Act, which despite its name actually allows Banks to supply law enforcement agencies to access bank records related to suspicious activities in general and any transaction exceeding $10,000. Such information is invaluable to the US Customs Service and the FBI in tracking money-laundering operations that often the involve illegal drug trade. Opponents such as the ACLU argue that such laws violate the Fourth Amendment of the US Constitution banning unreasonable search and seizure.

Date 1999-04-20 **Keyword** airline passenger screening terrorists

Source, Vol, No. Wired

The new Federal Aviation Agency supersecret passenger profiling system will watch for patterns of ticket purchase and other travel behavior correlated with terrorism and crime. Declan McCullagh wrote in _Wired_ that terrorist profiles include "a passenger's last name, whether the ticket was purchased with cash, how long before departure it was bought, the type of traveling companions, whether a rental car is waiting, the destination of the flight and passenger, and whether the ticket is one-way or round-trip." Privacy advocates, including the ACLU, argued that the U$2.8B system proposed in 1997 would inevitably infringe on personal freedom and likely begin to use race and ethnicity as factors despite explicit exclusion from the initial algorithms.

Date 1999-04-20 **Keyword** Internet privacy law legislation bill children FTC Web

Source, Vol, No. ZDNN

The Federal Trade Commission announced a notice of proposed rulemaking implementing the Children's Online Privacy Protection Act of 1998. The law takes effect in 2001. The proposed implementation would require all Web sites soliciting or collecting information from children under 13 years of age to obtain explicit permission from the children's parents or guardians. How exactly such a scheme could possibly be implemented without strong identification and authentication and verifiable digital signatures remained a complete mystery.

Date 1999-04-20 **Keyword** privacy personal information protection law bill act Europe

Source, Vol, No. Wired

Canadian legislators moved quickly to conform to the European Union Data Privacy Directive. The Personal Information Protection and Electronic Documents Act C-54 would provide consumers with considerably more control over the way data about themselves could be collected and used. US delays in conforming to the Directive threatened international trade with Europe and other collaborators in the effort to increase privacy.

Date 1999-04-21 **Keyword** privacy seal certification online Internet Web credit report

Source, Vol, No. CNET News.com <http://www.news.com/News/Item/0,4,35487,00.html>

A firestorm erupted when the Better Business Bureau Online granted a seal of approval to Equifax, a major credit-rating agency that has been the bête noire of the privacy lobby for years. Critics pointed out that both the BBB Online and Truste seals refer exclusively to Web sites and ignore privacy violations carried out by firms using other modalities.

Date 1999-04-22 **Keyword** privacy law Canada European Privacy Directive bill proposal

Source, Vol, No. National Post (Canada) editorial

An editorial by Richard C. Owens in Canada's right-wing, business-oriented _National Post_ newspaper criticized Bill C-54, the Personal Information Protection and Electronic Documents Act, claiming that "If passed and enforced, this law will impede transactions and lower asset values across the country." The writer argued that restrictions on sale of customer or prospect databases as part of the assets of a company would lower the value of companies; that inability to exchange information would harm outsourcing; and that the law addresses a problem that looms large in the public mind but is in fact a minor issue in practice.

Date 1999-04-29 **Keyword** EU data privacy directive US compliance government law

Source, Vol, No. COMPUTING (UK)

At the end of April, the US Department of Commerce announced principles for US companies to comply with the European Union Data Privacy Directive. An article in the British magazine _Computing_ said, "Under the principles, organisations are required to tell individuals about the information held on them; allow individuals to choose how that information is used, including onward transfer; and maintain secure systems to ensure data integrity, allowing access to their systems for enforcement of these principles. Organisations will be permitted to use private sector programs to ensure compliancy with the agreement. However, these must include effective enforcement and dispute resolution with either supervisory authorities, or via co-operation with data privacy organisations in the EU."

Date 1999-04-29 **Keyword** Pentium serial number Trojan diagnostic Intel vulnerability

Source, Vol, No. New York Times

Intel admitted that its Pentium III processors included a unique serial number accessible to software. The Montreal company that disclosed the processor numbering, Zero-Knowledge Systems, became the target of a mild form of information warfare when Intel executives persuaded leading anti-virus software maker Symantec (of Norton Anti-virus fame) to define the Z-KS demo program as hostile code.

Date 1999-04-29 **Keyword** corporate privacy policy requirements EU directive compliant

Source, Vol, No. Computer Weekly (UK)

David Bicknell, writing in the UK's _Computer Weekly_, urged IT directors to study the new European Data Privacy Directive and implement privacy-compliance changes to prevent expensive fines and loss of business for their employers. The deadline for compliance in the UK is the end of 2000, so experts are advising Y2K teams to attack privacy as soon as the Y2K issue is solved.

Date 1999-05-04 **Keyword** privacy proposal bill Administration fraud banking transactions sharing

Source, Vol, No. Washington Post < http://www.washingtonpost.com/wp-srv/business/daily/may99/privacy4.htm >

In May, the Clinton Adminstration proposed a bill to protect personal records of financial and medical information. The proposal included $5M for training law enforcement personnel in fighting securities fraud and for increased surveillance of the Internet.

Date 1999-06-22 **Keyword** advertising marketing privacy policy Web

Source, Vol, No. AP

Microsoft announced that it would no longer place Web ads on sites that failed to provide acceptable privacy policies starting in the year 2000.

Date 1999-08-16 **Keyword** privacy anonymity Web cloaking encryption cookies concealment law enforcement warrants

Source, Vol, No. New York Times

Privada announced a new anonymizing service for $5 a month; the service would use the company's servers as proxies for all Internet access and add encryption and protection against tracking through cookies. The company also asserted that it would respond to law enforcement warrants. "Our service is for protecting the privacy of consumers, not for hiding criminals or criminal activities," said CEO Barbara A. Bellissimo.

Date 1999-10-01 **Keyword** survellance privacy law enforcement wiretaps guards police detection

Source, Vol, No. WEST AUSTRALIAN

The Research Director of the Australian Institute of Criminology, Peter Grabosky, gave a pessimistic view of the future in his keynote speech at the Annual Conference of the Australia and New Zealand Society of Criminology held at the University of Western Australia in September. Decreasing budgets for police, the increasing use of private security forces and public pressure to find and punish drug-dealers and other malefactors was already contributing to a climate that was more tolerant of surveillance than in the recent past.

Date 1999-10-07 **Keyword** online privacy seals certification complaints investigation Web

Source, Vol, No. ZDNet

The FTC announced a new policy on consumer complaints about privacy violations on the Net. Any complaint received from the privacy certification groups (e.g., Truste) will be passed to FTC investigators immediately. However, in a related story, EPIC (The Electronic Privacy Information Center) asked the FTC for a list of the privacy investigations in June; when none were forthcoming by October, EPIC sued in order to get the data they needed for an analysis of FTC effectiveness in pursuing such complaints. The FTC protested that they needed to anonymize the data to protect the complainants' and accuseds' privacy.

Date 1999-10-21 **Keyword** children privacy parental approval authorization data collection Web

Source, Vol, No. New York Times

The FTC defined new rules controlling data collection from and about children on the Web. Depending on the nature of the interaction, parental authorization could be defined by the increasingly stringent requirements for postal mail, fax, credit card, or digital signatures.

Date 1999-11-03 **Keyword** privacy monitoring playlist music recording interest aggregate data mining policy disclosure scan

Source, Vol, No. Wired, RealNetworks < http://www.real.com/company/pressroom/pr/99/updateadvisory.html >

RealNetworks admitted that it had been collecting information about exactly what its users of RealJukebox player had been listening to. The company did not inform its users of the monitoring and got hammered by its competitors, privacy advocates and many users. The company immediately changed its public privacy statement to let people know about the data collection function and its spokesperson swore that the data had been aggregated so that no one could trace the specific interests of any one user. The company immediately apologized to the public for the concerns it had caused and provided a patch to disable detailed reporting. The company's statement included the following text:

This RealJukebox update causes the following changes to the product:

The RealJukebox globally unique identifier (GUID) is now disabled, and is set to zeros for all users. As a result, GUIDs cannot be associated with any personal registration information (such as name and e-mail) that you may have given RealNetworks.

Since the RealJukebox GUID is disabled and set to zeros, it no longer contains any reference to the network card MAC address of the user's computer.

The following information will no longer be sent during the Get Music service update:
- Encoding options
- Portable devices
- Total song tracks in music database (recorded and downloaded)
- Total recorded song tracks in music database (recorded only)
- User option to receive automatic music downloads (set to blank)
- Genre preference A unique RealJukebox ID will no longer be sent during requests for CD information.

Date 1999-11-03 **Keyword** privacy financial services banking customer confidentiality legislation law bill

Source, Vol, No. EPIC Alert 6 18

At the beginning of November, the Financial Services Modernization Bill of 1999 (S. 900) obliged financial institutions to disclose their privacy policies to consumers and restricted release of account numbers and access codes to third parties. However, the bill did not require explicit consent before allowing disclosure of a customer's financial information to third parties such as marketing agencies. The legislation did not override better privacy protection at the state level.

Date 1999-11-19 **Keyword** privacy communications wiretapping law enforcement interception monitoring

Source, Vol, No. EPIC

On November 19th, EPIC and the ACLU issued a press release that began as follows:
The Electronic Privacy Information Center (EPIC) and the American Civil Liberties Union (ACLU) today asked a federal appeals court to block new rules that would enable the FBI to dictate the design of the nation's communication infrastructure.

The challenged rules would enable the Bureau to track the physical locations of cellular phone users and monitor Internet traffic. In a petition to the U.S. Court of Appeals for the District of Columbia Circuit, the groups say that the rules — contained in a Federal Communications Commission (FCC) decision issued in August -- could result in a significant increase in government interception of digital communications.

The court challenge involves the Communications Assistance for Law Enforcement Act ("CALEA"), a controversial law enacted by Congress in 1994, which requires the telecommunications industry to design its systems in compliance with FBI technical requirements to facilitate electronic surveillance. In negotiations over the last few years, the FBI and industry representatives were unable to agree upon those standards, resulting in the recent FCC ruling. EPIC and the ACLU opposed the enactment of CALEA in 1994 and participated as parties in the FCC proceeding.

Date 1999-11-24 **Keyword** banner advertisements data capture privacy surveillance Web Internet license software freeware

Source, Vol, No. ZDNet < http://www.zdnet.co.uk/news/1999/46/ns-11692.html >

Conducent <http://www.conducent.com> pays software developers to include modules in their programs that display banner ads. A contributor to the RISKS Forum, Bill Royds, reported that the modules initiate a TCP/IP connection to Conducent computers and report on which program is running and other information about the user's system such as IP address. In addition, the reporting module responds to connection failure (e.g., through firewall restrictions) by initiating a storm of connection attempts (10 per second). Conducent responded dismissively that their licenses are clear and said, "It is up to the user to take the time to read the installation notes wherein the advertising-supported version of the software is explained comprehensively."

Date 1999-11-30 **Keyword** Trojan program privacy invasion reporting TCP/IP Internet browsing statistics visit sites advertisi

Source, Vol, No. AP

Comet Systems Inc's cute cartoon cursors were downloaded by millions of people, many of them children. However, the free software turned out to be a Trojan: the modified programs initiated TCP/IP communications through the users' Internet connections and reported on which sites were being visited by each copy of the programs when the users went to any of 60,000 sites providing links to the cursor programs. Purpose: gathering statistics about Web usage patterns. Company officials argued that there were no links between the serial numbers and any identifying information about the users.

Date 1999-12-06 **Keyword** privacy cookies Web e-mail Trojan vulnerability tracking covert

Source, Vol, No. USA Today

Computer scientist Richard S. Smith (famous in part for helping to unmask David L. Smith, the author of the Melissa virus) discovered that popular e-mail clients such as MS-Outlook and Netscape Messenger allow anyone to send a victim a concealed cookie via e-mail that will then allow tracking through the Web as the cookie-infested user browses various sites. Privacy groups including the Center for Media Education, the Consumer Federation of America, the Electronic Frontier Foundation, the Electronic Privacy Information Center, Junkbusters, Privacy International, and Ralph Nader's Consumer Project on Technology all protested the covert use of this technology. Microsoft and Netscape announced that they would plug this security hole in their products.

Date 1999-12-06 **Keyword** information warfare privacy government international spying NSA

Source, Vol, No. Newsbytes, Wired, Security Wire

The American Civil Liberties Union (ACLU) announced formation of Echelonwatch.org in cooperation with the Electronic Privacy Information Center (EPIC) and the Omega Foundation to monitor developments in the controversial Echelon spy network. According to the ACLU and others, the Echelon program is an effort to filter out potential national and international security threats from all kinds of global communications, including wire, satellite, microwave, and wireless channels. There are few details available, since the National Security Agency (NSA) refuses to discuss the project in public. It is theorized that the system analyzes voice and data to spot keywords that alert observers to possible threats. On December 3rd, EPIC filed a lawsuit against the NSA demanding access to government documents about Echelon.

Date 1999-12-15 **Keyword** surveillance artificial intelligence pattern recognition speech keywords NSA ECHELON

Source, Vol, No. Crypto-gram 99 12

The ECHELON system was described in a report by Bruce Schneier in his Crypto-gram newsletter for December 1999 < http://www.counterpane.com/crypto-gram-9912.html >. He wrote, "I've seen estimates that ECHELON intercepts as many as 3 billion communications everyday, including phone calls, e-mail messages, Internet downloads, satellite transmissions, and so on. The system gathers all of these transmissions indiscriminately, then sorts and distills the information through artificial intelligence programs. Some sources have claimed that ECHELON sifts through 90% of the Internet's traffic. " Apparently some recent patents filed by the NSA detail algorithms for rapid recognition of keywords in phone message and Internet traffic.

Date 1999-12-21 **Keyword** Echelon government spying surveillance intelligence exchange law privacy criminals

Source, Vol, No. < http://www.datashopper.dk/~boo/index.html >

Investigative reporters Bo Elkjaer and Kenan Seeberg of Denmark published several dozen reports in Danish about the Echelon spy network. They interviewed reclusive communications engineer Margaret Newsham in a Las Vegas suburb, where the ex-Lockheed Martin employee lives alone with an attack-dog and sleeps with a loaded pistol under her pillow — in fear, she says, of retaliation by the US intelligence services for her blowing the whistle on Echelon. Ms Newsham says that she was directly involved in the creation of the worldwide surveillance systems and was fired in 1984 for protesting the direction of the project. She told the reporters that the projects she worked on from 1974 to 1984 involved remote surveillance by the CIA and NSA of US citizens who were on US soil — a clear violation of US law.

Category 4A Evolution of Net law: framing, pointing, linking, jurisdiction

Date 1999-02-11 **Keyword** information warfare competition advertisements Web sites intellectual property copyright

Source, Vol, No. Reuters

In a striking example of information warfare, the Alexa Internet company offers competitors the opportunity to superpose their own ads on top of their competition's Web pages. Subscribers to the Alexa service get "smart links" which provide pop-up information such as a Web site's company address and financial information. In addition, the service allows advertisements to be tailored to a specific target; for example, ads can appear when the user clicks on a competitor's Web site.

Date 1999-04-19 **Keyword** law regulation Web site universal readability access

Source, Vol, No. Freedom Forum <http://www.freedomforum.org/technology/1999/4/30handicapaccess.asp>

According to the US Access Board, established to enforce the Disabilities Act of 1990 and other equal-opportunity legislation, all federal government Web sites will have to provide for accessibility to visually-impaired users in compliance with Section 508 of the 1998 Workforce Investment Act. The deadline for government sites was the end of May 1999; by 7 Aug 2000 the requirements will extend to suppliers with federal contracts. According to some members of the federal Electronic and Information Technology Access Advisory Committee, the same rules will eventually apply to all Web sites hosted in the USA. Requirements stipulate that "in addition to conventional html and PDF versions available online, all online information must also be available from the agency via audio text and TTY, as well as through cassette tape, Braille, large print, or computer disk."

Date 1999-04-28 **Keyword** e-mail spam mail-bombing civil lawsuit injunction

Source, Vol, No. AP, Los Angeles Times < http://www.latimes.com/home/business/t000038417.html >

In 1995, Intel employee Ken Hamidi was fired; he responded by flooding Intel with critical e-mail to 30,000 of his former colleagues at Intel. The company obtained an injunction in April 1999 to stop Hamidi from sending his message to corporate e-mail accounts. Free-speech advocates were shocked at the judge's decision that the company's e-mail system, even though connected to the Internet, was not a public forum and that Hamidi's unauthorized use of the addresses constituted illegal trespass.

Date 1999-05-11 **Keyword** e-commerce law legislation regulation Europe international

Source, Vol, No. E-Commerce Times

The European Commission approved several measures affecting e-commerce: (1) jurisdiction over electronic transactions would reside in the country of the seller; (2) consumers would have a single European opt-out registry to escape spam; (3) ISP liability for copyright violations and libel would increase; (4) ISP liability for third-party storage and transmission of illegal content would be reduced.

Date 1999-05-13 **Keyword** Internet Web advertising regulation enforcement policing FTC

Source, Vol, No. E-Commerce Times

A predictable burst of protest met the modest proposals from the FTC to monitor online advertising to cut down on fraud. Large ISPs such as AOL and the ITAA (Information Technology Association of America) claimed that the move was too regulatory.

Date 1999-05-17 **Keyword** Web online publishing annotation comments free speech

Source, Vol, No. Wall Street Journal

An interesting wrinkle in the on-going fights over second-hand representation of Web-site content erupted when Third Voice announced a new service allowing participants to post and see the electronic equivalent of "Post-It" notes on any Web site — without the involvement or approval of the Web-site owners. The notes look like part of the original site to the uninformed.

Date 1999-06-09 **Keyword** jurisdiction Internet Web servers state location physical presence lawsuit

Source, Vol, No. C|NET

The three judges of the California Court of Appeal for the Second District ruled that the mere physical presence of servers hosting a Web site does not constitute grounds for defining jurisdiction. The case was Rambam vs the Jewish Defense Organization; plaintiff argued that because the JDO used California-based GeoCities and Xoom.com servers to host their Web site, therefore he should be able to sue defendant in California.

Date 1999-06-14 **Keyword** privacy defamation anonymity Internet Web law tort lawsuits

Source, Vol, No. LA Times

Companies being attacked by anonymous critics online began suing "John Doe" defendants and demanding that the courts force disclosure of the identity of their gadflies. Xircom attacked someone called "A View From Within" for his or her criticism of the company. In the first six months of 1999, AOL alone was served with 110 warrants for disclosure of users' actual identities.

Category 4B Intellectual property: patents, copyrights (law)

Date 1999-01-05 **Keyword** trademark lawsuit judgement injunction phrase words

Source, Vol, No. AP

AOL sued AT&T for daring to announce "You have mail" to its e-mail users. The largest ISP in the world argued that it should have exclusive right to utter those words in an online session. On Christmas eve 1998, U.S. District Judge Claude Hilton (Alexandria, VA) declined to issue an injunction against such use, although he did permit the case to go to court.

Date 1999-02-05 **Keyword** copyright law distance education publishers entertainment

Source, Vol, No. Chronicle of Higher Education

At a hearing in February before the U.S. Copyright Office, educators lobbied for the right to use copyrighted works in their distance-education programs offered via the Internet without having to obtain explicit permission from the copyright owners. Their position was vigorously opposed by publishers and by speakers for the entertainment industry.

Date 1999-02-11 **Keyword** copyright trademark infringement search engines pornography

Source, Vol, No. USA Today

John Gehl and Suzanne Douglas, editors of EDUPAGE, wrote with their usual admirable conciseness about a potentially crucial case in the evolution of Internet law: "Playboy Enterprises is suing portal sites Excite and Netscape for trademark infringement because searches on words trademarked by Playboy, such as `Playboy' and `Playmate,' turn up banner ads for a cluster of hard-core porn sites that are benefiting from a misappropriation of Playboy's `good will and reputation.' "

Date 1999-03-12 **Keyword** industrial espionage intellectual property lawsuit court

Source, Vol, No. SJ Mercury News

In an unusual attempt to extend the anti-compete clauses of many employment contracts in the high-tech fields, Motorola applied to a court for injunctions preventing Intel from hiring ex-employees of Motorola. [Perhaps corporations will someday apply electroconvulsive shock treatments -- excellent for causing amnesia -- to its best minds when they leave.]

Date 1999-03-19 **Keyword** intellectual property database piracy appropriation law bill

Source, Vol, No. New York Times

A proposed bill introduced in the US Congress by Rep. Howard Coble (R--NC) would protect the interests of database compilers and backed by the Coalition Against Database Piracy lobbying group. Many forces opposed the bill, including the Clinton administration, many academics, Internet service providers, bankers, and medical organizations. The opponents argue that the bill could severely interfere with the free exchange of publicly available information.

Date 1999-05-03 **Keyword** copyright music copying illegal intellectual property license player MP3 G2

Source, Vol, No. New York Times < http://www.nytimes.com/library/tech/99/05/biztech/articles/03real.html >

RealNetworks announced that its Real Jukebox software includes copy protection — of a sort. An electronic "tether" warns the user that attempts to copy a downloaded audio CD file on a different computer is a violation of copyright. Because the tether can easily be disabled or ignored, the music industry was not impressed.

Date 1999-05-03 **Keyword** music Web intellectual property copyright MP3 recording

Source, Vol, No. New York Times

Real Networks announced in early May that its new streaming player, Real Jukebox, would allow users to download and store a variety of digital audio formats, including MP3 and the company's own G2 files. In a weak nod to copyright concerns, the software includes an optional feature to limit the number of copies to be stored on disk.

Date 1999-05-04 **Keyword** copyright intellectual property e-commerce protection encryption software music MP3

Source, Vol, No. Los Angeles Times <http://www.latimes.com/home/business/t000040006.1.html >

InterTrust Technologies launched a copy-protection scheme with Seagram's Universal Music Group in May. The DigiBox system encrypts data of any kind for download to users and offers options such as allowing a brief sampler of a music track or charging a minor fee for a day of listening or of usage before the buyer decides whether to buy that product.

Date 1999-05-28 **Keyword** intellectual property universities schools colleges copyright Fair Use Doctrine education non-com

Source, Vol, No. Wired

The U.S. Copyright Office released recommendations urging that public schools and universities be granted exemptions under Fair Use doctrine for educational, non-commercial use of copyright materials.

Date 1999-06-22 **Keyword** reverse engineering trade secrets copyright infringement security analysis WIPO treaty law propo

Source, Vol, No. PC Week < http://www.zdnet.com/pcweek/news/0622/22wipo.html >

The World Intellectual Property Organization (WIPO) treaty that was passed by the Senate of the United States in May would have serious consequences for consumers and for security experts. The treaty would render reverse engineering of proprietary software and ban real-world testing of security software.

Date 1999-07-26 **Keyword** chat instant message proprietary protocol reverse engineering conflict breach

Source, Vol, No. Washington Post < http://washingtonpost.com/wp-srv/WPlate/1999-07/28/118l-072899-idx.html >,

AOL did not take kindly to attempts to make other products compatible with its proprietary Instant Messenger software. The company immediately changed its protocols when Microsoft, Yahoo! And Prodigy attempted to allow their users to communicate with AOL users using chat-popup boxes. AOL even hinted that just trying to chat with its users was a breach of security. Within a few days of the start of the blowup, though, AOL began cooperating with Apple Computer to provide precisely this functionality. In August, Microsoft tried to pressure AOL into cooperating by releasing the code for its own MSN messaging service, hoping thereby to influence the IETF (Internet Engineering Task Force) working group choosing a standard for instant Internet messaging.

Date 1999-07-29 **Keyword** software license restrictions anti-virus virus copyright reverse engineering testing commercial law

Source, Vol, No. Red Rock Eater News

In July, the National Conference of Commissioners on Uniform State Laws (NCCUSL) approved the controversial UCITA (Uniform Computer Information Transactions Act) proposal that would create common licensing rules for software and other IT transactions. The law applies to product
licenses and covers all aspects of modern IT, including data, databases, multimedia files, online transactions and software licenses. Among other protections for vendors, the UCITA provides for
* rigid enforcement of shrink-wrapped licenses even though the buyer may not see or agree to the terms until after the software has been purchased;
* banning reverse engineering of proprietary software;
* allowing vendors to shut down software remotely if they suspect a violation of the licensing terms;
* easier disclaimer of written warranties.
On 1999-06-10, the Business Law Section of the American Bar Association issued a blistering attack on the proposal. Staff of the Federal Trade Commission also submitted a brief opposing the UCITA on grounds of consumer protection and potential damage to competition. The ACM strongly opposed the proposal, and its President commented that theoretically, the UCITA would make anti-virus software illegal because viruses, which are automatically copyrighted by their authors, could no longer be reverse engineered. The Newspaper Association of America and the Magazine Publishers of America also formally opposed the UCITA, saying that the proliferation of different state rules on intellectual property would make their operations unwieldy by distinguishing between print and online media.

Date 1999-09-28 **Keyword** copyright writers publishers legal case conflict rights royalties CD-ROM

Source, Vol, No. Newsbytes

A New York state court ruled in favor of the National Writers Union and against the New York Times and other major publishers in defending the right of writers to control publication of their materials on new media. The publishers wanted to use submissions on CD-ROMs or on the Web without paying additional royalties.

Date 1999-10-16 **Keyword** patents Internet operations methods innovations

Source, Vol, No. New York Times, Computerworld, New Scientist

In 1998, the U.S. Patent and Trademark Office granted 125 patents for online business practices and was expected to issue up to 200 in 1999. Critics suggest that some of these patents merely appropriate common non-electronic ways of doing business; e.g., <Priceline.com> patented the reverse auction, where vendors offer their best price to customers asking for products or services. Such patents are unlikely to be enforceable, according to intellectual-property-law specialists.

Date 1999-11-26 **Keyword** intellectual property control license screen copy-protection print

Source, Vol, No. OTC

BreakerTech, a UK company, announced its new SoftSEAL technology for preventing computer users from using screen-capture commands to foil intellectual property restrictions.

Date 1999-12-07 **Keyword** counterfeits intellectual property products

Source, Vol, No. Times of London

Hasbro, a major toy and game manufacturer, declared war against counterfeiters in December. The company launched a vigorous advertising campaign and arranged for increased cooperation with law enforcement to crack down on companies illegally making unauthorized copies of such popular items as Action Man, Furby, Monopoly and Pokemon.

Category 4C Security paradigms, risk management, site-security certification

Date 1999-01-05 **Keyword** computer emergency response team CERT

Source, Vol, No. South China Morning Post

The Hong Kong Internet Service Providers Association (HKISPA) and the Hong Kong Productivity Council (HKPC) began seeking government funding to create a local branch of the Computer Emergency Response Team (CERT).

Date 1999-02-12 **Keyword** text book overview introduction paradigm model management

Source, Vol, No. RISKS 20 21

Rob Slade reviewed Donn B. Parker's new (1998) book, _Fighting Computer Crime_ (John Wiley & Sons, ISBN 0-471-16378-3). He wrote, "Parker's stance on security in general definitely puts him in the camp of the professional paranoids. However, absent the first and last chapters, there is a lot of good, solid knowledge here to help educate any security practitioner."

Date 1999-02-20 **Keyword** site-security certification information warfare consultants

Source, Vol, No. National Post (Canada)

James Adams of IDefense Corp (Washington, DC) announced a site-security certification seal. He said, "We are Dun & Bradstreet meets the CIA meets the stamp of Good Housekeeping approval. We the only one in the world like it. There will be others but that's okay. Competition is good." [Yes, especially since the TruSecure seal from ICSA.net was on the market in 1998.]

Date 1999-04-24 **Keyword** certification standards Internet perimeter scan

Source, Vol, No. BSI PR

In April, the British Standards Institute announced the release of a new version of its successful BS 7799 standards and of the C:CURE security certification scheme. The update cost £94 (£47 to BSI members), and could be ordered from BSI Customer Services, 389 Chiswick High Road, London W4 4AL, England. Phone: 0181 996 9001, fax: 0181 996 7001, email: <info@bsi.org.uk>, website: <www.bsi.org.uk>. The C:CURE certification scheme information was available from BSI DISC, 389 Chiswick High Road, London W4 4AL, England. Phone: 0181 996 7799, fax: 0181 996 6411, email: <c-cure@bsi.org.uk>, website: <www.c-cure.org>.

Date 1999-04-26 **Keyword** theft law enforcement deterrence detection forensics

Source, Vol, No. JOURNAL OF COMMERCE

Computer crime and theft of high-tech components cost a lot not only to the victims but also to law enforcement agencies forced into expensive and lengthy investigations and court cases. The San Jose Police Department decided to use a bit of outreach in a bid to reduce vulnerability to high-tech crime. A four-person squad operates a computer forensics laboratory that helps in investigations of all sorts where computer data are part of the evidence; the members also visit local industries to point out vulnerabilities and encourage tighter physical and computer security. The officers encourage insurers to push prevention as an important tool: "We don't have all the answers," Lieut. Stephen Ronco, commander of the unit, said. "But if underwriters can go back to their respective clients and simply ask them, how are you preventing such crimes, are your inventory audits tight, do you have security measures and other anti-theft policies in place to give guidance to supervisors and employees, it would help enormously."

Date 1999-04-29 **Keyword** vulnerability analysis certification BS7799

Source, Vol, No. Accountancy Age (UK)

Accountancy Age (UK) published an interesting article on the value of security standards such as the newly revised BS 7799 and independent vulnerability assessments such as the British Standards Institute's C:CURE in April. Experts insisted that security policy is a necessary prerequisite for any kind of certification and that policy is not a "techie" issue but a business management issue.

Date 1999-05-06 **Keyword** information warfare critical infrastructure certification

Source, Vol, No. Computing (UK)

In Britain, national security officials suggested that experts from the private sector ought to help protect the critical infrastructure of the UK. In August, the Communications Electronic Security Group (CESG) security agency launched a security audit called "IT Health Check." Companies approved by CESG and the Defence Evaluation Research Agency (DERA) would test computers and networks in the private sector for vulnerabilities and then provide recommendations for improvements.

Date 1999-07-20 **Keyword** telecommuting data communications encryption authentication digital signatures

Source, Vol, No. Washington Post

If Rep. Frank Wolf's (R-VA) proposed bill encouraging telecommuting were to become law, companies would earn pollution credits for the person-miles eliminated by allowing workers to stay at home while doing their jobs. These credits would be traded openly. In addition, if the 40% of 133M workers who could do their jobs from home offices did stay there, businesses could save millions in reduced office leasing, maintenance, heating, air-conditioning and lighting costs. [Yes, and if this actually does happen, we had better have really good security in place to protect data communications from breaches of confidentiality, integrity and authenticity. Virtual private networks and digital signatures, anyone?]

Date 1999-10-01 **Keyword** cybercops cyberpolice investigators

Source, Vol, No. Wall Street Journal

Dean Takahashi of the Wall Street Journal wrote an interesting and laudatory article about Dave Kennedy and his IS/RECON team, who scour the Net looking for criminal hacker activity. Full-time operatives also infiltrate criminal hacker groups and warn potential victims of pending attacks whenever possible.

Date 1999-10-02 **Keyword** bank financial systems security network alerts warnings sharing cooperation private

Source, Vol, No. AP

The US banking industry responded to President Clinton's demand for improved resistance to fraud in the financial sector. The Financial Services Information Sharing and Analysis Center was announced by the Treasury Department; its physical location was secret. The network will facilitate information sharing with full anonymity. According to Ted Bridis, writing for Associated Press, "Similar centers are planned in the coming months for seven other industries, including telecommunications, oil and gas, electrical power, transportation and America's water supply system."

Date 1999-10-05 **Keyword** security-enabled e-business SEE Entrust paradigm encryption keys banks

Source, Vol, No. Entrust <http://www.entrust.com/news/1999/09_21_99.htm>, American Banker

Entrust Technologies Inc.'s President and CEO, John Ryan, published a white paper on "security-enabled e-commerce" <http://www.entrust.com/downloads/see.htm>. The paper recommends that security be integrated into the business planning cycle for Internet-based commerce and provides a good management overview of some of the technical means for assuring security while enhancing competitive position and profitability.

Date 1999-10-11 **Keyword** e-commerce security alliance group industry consortium

Source, Vol, No. New York Times

In October, Compaq Computer, Hewlett-Packard, IBM, Intel and Microsoft formed the Trusted Computing Platform Alliance to develop universal security standards for e-commerce and to improve the security of personal computers.

Date 1999-10-15 **Keyword** taxonomy classification terminology vulnerabilities database

Source, Vol, No. < http://www.mitre.org/news/articles_99/cve_release.shtml >

MITRE Corporation announced the Common Vulnerabilities and Exposures (CVE) database, in which over 300 vulnerabilities are cross-indexed so that security experts and security-product developers can figure out which vulnerabilities and exposures they are talking about.

Date 1999-10-18 **Keyword** conference data sharing information pooling computer crime defense vulnerability database

Source, Vol, No. San Jose Mercury News Online

At the 22nd National Information Systems Security Conference organized in Arlington, VA by the NIST (National Institute of Standards and Technology) and the NCSC (National Computer Security Center), panelists urged industry and government to pool knowledge about security threats and vulnerabilities to strengthen the Good Guys' hands against computer criminals.

Category 4D Funny / miscellaneous

Date 1999-01-04 **Keyword** stupidity satellite navigation automobile user error

Source, Vol, No. RISKS 20 14

In a spectacular demonstration of slavish obedience, a pair of nitwits demonstrated the crucial role of observation and thought when using mission-critical technology. Peter G. Neumann wrote, "A German couple drove their BMW with great confidence under control of its computerized satellite navigation. Indeed, they drove it past a stop sign, down a ferry ramp, and into the Havel River in Caputh, near Potsdam/Berlin, Germany. The computer system reportedly neglected to tell them they needed to wait for the ferry. Ship traffic was stopped for two hours, but the couple was OK.

Date 1999-01-15 **Keyword** data leakage covert channel recording eavesdropping toy

Source, Vol, No. RISKS 20 16

The electronic stuffed toys called Furbys were declared machina non grata at government installations when the NSA realized that the little devils could record human speech and play it back. RISKS correspondent Bruce Martin wrote (in issue 20.16), "The risk of U.S. national security resting in the hands of adults who play with children's toys during office hours is left as an exercise to the reader."

Date 1999-01-25 **Keyword** operating system refund complaint UNIX PCs

Source, Vol, No. New York Times

A group of LINUX users announced plans to demand refunds from Microsoft because they were charged for unwanted installations of MS-Windows on PCs sold by various vendors. Microsoft frostily replied that there would be no refund.

Date 1999-02-12 **Keyword** software law legal interference judge court case self-help

Source, Vol, No. RISKS 20 21

Peter Neumann wrote in RISKS: "U.S. District Judge Barefoot Sanders is moving to ban the sale of self-help legal software such as Quicken Family Lawyer." [What more need one say?]

Date 1999-02-22 **Keyword** jargon English style punctuation capitalization newspspeak

Source, Vol, No. SYDNEY MORNING HERALD (Australia)

John Huxley wrote an amusing article for the Sydney Morning Herald of Australia on the growing use of computer jargon in Silicon Valley and elsewhere. Some of his observations on new fashions in writing and speaking:
* being out of personal bandwidth.
* writing entirely in lowercase and without punctuation.
* use of abbreviations such as the "@" symbol and acronyms such as IMHO (In my humble opinion), OTOH (On the other hand), and G,D&R (Grin, duck and run).
* emoticons :-) (and one of Dave Barry's better gags, :-(8 — a person who is unhappy with the results of breast-enlargement surgery.
* Spammers = senders of unsolicited email.
* Marketing pukes = salespeople who know buzzwords but little else.
* Ponytails = artistic or creative people.
* SLIRKs = Smart Little Rich Kids — successful entrepreneurs or techno-criminals.
* WOMBATS = people who are a Waste of Money, Brains and Time.
* PEBCAK = Problem Exists Between Chair And Keyboard.
* FRED = Fucking Ridiculous Electronic Device.

Date 1999-03-08 **Keyword** stupid laws privacy regulations copyright download caching

Source, Vol, No. LA Times

In a spectacularly stupid move, the European Parliament issued a directive forbidding disk caching of Web pages. Any ISP serving European users would be banned from applying this simple technique, thus forcing a significant increase in bandwidth utilization and undoubtedly slowing access to all sites on the Net for everyone, not just Europeans. Internet Society CEO Don Heath commented, "The Internet does not need laws that slow its performance, clog its arteries and reduce value received," noting also that HTML already provides mechanisms for preventing caching of specific pages.

Date 1999-05-05 **Keyword** spoof virus spellcheck funny

Source, Vol, No. Washington Post

Bob Hirschfeld published an amusing spoof in the Washington Post in May 1999 in which he claimed that a new virus was paralyzing government and business by blocking ungrammatical e-mail."

Date 1999-10-03 **Keyword** CIA government investment

Source, Vol, No. Philadelphia Inquirer, New York Times, Washington Post

The CIA announced its new venture capital firm, In-Q-It, to funnel funds into high-tech firms. CEO Gilman Louie has no known experience in espionage or security; however, he did found a toy company later acquired by Hasbro.
