Widow

Next Issue. The deadline for the next issue is 21 Jun 1993. Thanks. Peter G. Neumann

RISKS TO THE PUBLIC IN COMPUTERS AND RELATED SYSTEMS

Peter G. Neumann, Moderator

[*SEN* Editor and Chairman of the ACM Committee on Computers and Public Policy], plus contributors as indicated. Opinions expressed are individual rather than organizational, and all of the usual disclaimers apply.

Revenge via computer (From Thomas Dzubin)

A man sent his ex-wife (who had apparently asked him to retrieve some inaccessible files) a computer diskette that destroyed her entire hard disk, including software and manuscripts, and then displayed a vengeful limerick. James Welsh, a 32-year-old accountant, has pleaded not guilty to three counts of ''introducing a virus'' into the computer. He could face three years in prison if convicted. Welsh's ex-wife, writer Kathleen Shelton, said she had a problem with a computer they formerly owned together. Welsh apparently sent her a computer disk with instructions for correcting the trouble. Police said, ''She followed Welsh's instructions, which resulted in the destruction of approximately $8,000 worth of software and manuscripts, leaving only [an abrasive] limerick explaining Welsh's actions against her.'' Detectives searched Welsh's home, seized $4,000 worth of computer hardware and allegedly found evidence of the 'virus'. Welsh's lawyer, Annette Lombardi, said: ''There's not as much damage as charged. It's basically the cost of getting a guy to fix the computer and install new software.'' [Presumably a *different* guy this time..., maybe someone who can write poetry that scans, which the omitted limerick didn't. PGN, based on *The Province*, Vancouver, B.C. Canada and San Francisco Chronicle, 4 Dec 1992.]

Jail-Door Lock Problems

Around 7pm on 27 Dec 1992, the new San Joaquin (California) County Jail computer system automagically unlocked all of the cell doors in a high-risk area, with a highly audible series of loud clicks, releasing about 120 potentially dangerous inmates who were being held in an 'administrative segregation pod'. Fortunately, the pod was itself isolated by other doors that remained locked. The glitch was attributed to a spurious signal from the 'incoder card' whose responsibilities include opening those doors in emergencies. Also, less than a year after the supposedly escape-proof Pelican Bay State Prison near Crescent City CA opened, inmates learned how to pop open the pneumatic cell doors at will. A similar system in the Santa Rita Jail in Alameda County was also found to be pickable. [If it had required breaking DES, that situation might have been DES-pickable!] [Source: San Francisco Chronicle, 30 Dec 1992, p.A14, article by Peter Fimrite]

Oklahoma power outage freezes jail doors (Originally from Jennifer Smith)

Oklahoma County opened a new jail in November 1991, with a comprehensive new computer system developed in Colorado. Towards the end of February 1993, the software failed, leaving each of the doors in a state that could not be changed manually. Some prisoners remained locked in their cells, some doors remained wide open. Twenty-two jailers were trapped in a control room for an entire shift when the computer system shut down due to a five-minute power outage. An attempted fix four days later failed. [Source: New Software Fails to Fix Jail's Computer System, by Judy Kuhlman, Daily Oklahoman, 26 Feb 1993, contributed by Jennifer Smith, and summarized by PGN. Jennifer believes that this was the same allegedly 'escape-proof' jail that had 2 escapes within its first month of operation. ''Having computer-controlled doors with not even a surge protector, not to mention no one in the state running the system, is unfortunately quite typical.'' JS. RISKS previously reported the effects of a failure of automatic jail-doors in El Dorado, California, in ***SEN*** 13, 4, October, 1988. PGN]

Racetrack goes to the dogs as computer fails (Mark Colan via John Markoff)

BBC's NewsHour (heard on WBUR) mentioned an error in a betting computer at a greyhound race track. The computer continued to accept bets well after the conclusion of the race. Needless to say, many gleeful track-betters bought tickets for the dog that had already won, and claimed their winnings. The article also mentioned that some people are just born losers. After the race had finished, 139 people bet on dogs that had *lost*! The government management reported that they intended to reclaim all of the unfairly-won monies. However, they stated that they intend to *keep* the money from the losers. [JM]

Conrad Bullock responded to John Markoff's posting from New Zealand with several interesting observations, which are summarized here. The incident took place on 7 Jan 1993, involving the computer system run by the NZ Totalisator Agency Board (TAB) at the Waikato Greyhound Club meeting. Because of telecommunication difficulties, all races were being delayed by half an hour. However, the Waikato and Auckland site operators somehow had their computers believing the delay was one hour. Upon closing of betting after the half-hour delay, the computer balked with a 'Override for Early Close' error message, which the operator had never seen before, but the operator had already walked away and did not see the message for another three minutes. (The average race is over in about 20 seconds. Greyhounds are *fast.*) Bets were placed from all over the country in the interim. [The 139 bets on losing combinations were largely the result of people using a random selection (Easybet). The 'loss' was approximately NZ$7,000, of which NZ$5,000 was wagered at a single agency; the agent has been arrested, after allegedly placing bets him/herself and encouraging others to do so.]

Talk About Paying Through the Nose (From Jeffrey S. Sorensen)

Bill-collection agencies in England began lacing their invoices with a product containing androstenone, a chemical secreted from men's armpits and groins that is known to be a sex attractant in some species. In one preliminary study, mailed invoices treated with the product resulted in a 14 percent higher payment rate than untreated bills. [Jan/Feb 1993 issue of *Health* magazine, p. 53.]

The Less Care She Got, The Less She Cared (From Jeffrey S. Sorensen)

A patient in Manchester Royal Infirmary in England was found unconscious after she mixed up the nurse's call button with the one to give herself more painkiller and pressed the latter button impatiently for several minutes. [From the Art of User Interface design] (From Barry Salkin)

It is usual practice with Patient Controlled Analgesia (PCA) to have a lockout on the syringe driver, so that the patient cannot give themselves repeated doses without sufficient time between them. This not only prevents overdoses, but also means one bolus (dose) of painkiller has time to act before the patient is able to give themselves another dose, so that if the first dose is effective, the second, later, dose will not be administered by the patient. However, if the syringe driver wasn't set up with the time lockout, ...

Things that cannot possibly go wrong (From Pete Mellor)

The following extract from Douglas Adams' latest book *Mostly Harmless* (The fifth book in the increasingly inaccurately named *Hitch Hiker's Guide to the Galaxy* trilogy, Heinemann, London, 1992, ISBN 0434 00926 1) contains a lesson for designers of complex systems, particularly computerised ones (e.g., fly-by-wire): ''... all mechanical or electrical or quantum-mechanical or hydraulic or even wind, steam or piston-driven devices, are now required to have a certain legend emblazoned on them somewhere. It doesn't matter how small the object is, the designers of the object have got to find a way of squeezing the legend in somewhere, because it is their attention which is being drawn to it rather than necessarily that of the user's. The legend is this: 'The major difference between a thing that might go wrong and a thing that cannot possibly go wrong is that when a thing that cannot possibly go wrong goes wrong it usually turns out to be impossible to get at or repair.' ''

Bible belt broadcast bungle (From Peter J. Scott)

A major Christian radio network is alerting its member stations to check their latest shipments of religious compact discs before airing them. It seems that some other CDs were mislabelled at the factory and shipped along with the religious ones. Unfortunately the itinerant CDs were by the Dead Kennedys. A spokesman for the radio network said, ''This is what happens whenever people get around machines.'' The CBS newsreader, with masterful understatement, said, ''The Dead Kennedys CDs included songs such as, 'I Kill Children,' which some Christian listeners may not find inspirational.'' (Source: a radio broadcast on the morning of 28 Jan 93)

Computer error leaves Bundestag speechless (From Debora Weber-Wulff)

The German Bundestag, which had just moved into its brand-new, expensive quarters in Bonn (they'll be moving to Berlin someday, but this building was started when the Wall was still up), has been forced to move back into its old plenary building because of computer errors. The new building was installed with a special sound control system that was specifically designed to eliminate all the problems with feedback, screeching, volume adjustments and such that had plagued the old system. During the big budget debate (where the cost overruns in the new building were to be discussed as well :-) the sound system turned itself down to a whisper - no one could follow the speeches. After a 5 hour pause while technicians searched for the cause, the Bundestag moved back into the old building to resume the debates.

The cause: The architects had worked out an extremely symbolic form and used symbolic materials to create the building. The plenary chamber is round and completely enclosed in (bullet-proof) glass, to underline the transparency of the parliamentary process. This glass, however, does not absorb the sound, but rather it bounces it back. The computers, detecting feedback, turn down the volume to avoid this problem. A steady state is only achieved when the microphones are turned off. It will take until March to either replace the computerized system or put carpeting over the glass walls.

Seeing red over valentine envelopes (From Luis Fernandes)

Edmonton(CP)-- It's that time of year again when love is in the air and Canada Post is seeing red. Red envelopes, that is. That's because the computerized mail-sorting machines, which can process 33,000 letters an hour, have trouble reading addresses off the red envelopes popular for Valentine Day greetings, a Canada Post spokeswoman says. ''We in Canada have some of the most technically advanced machinery in the world,'' Teresa Williams says. ''And while it's not impossible for them to read red envelopes, some of them can present a bit of a challenge.'' If your valentine card hasn't arrived, it may have been delayed in the mail-sorting process, William says. A reminder for next year: white envelopes should be used instead. ''Or put a white sticker on a red envelope,'' Williams suggests. Meanwhile Hallmark Cards Inc., based in the United States, is complying with a U.S. Postal Service request to stop producing dark-colored envelopes over the next couple of years. U.S. machines can't read them either. [*Toronto Star*, 13 Feb 1993]

Solution found to risks of computers in elections! (From Jan I. Wolitzky)

According to the Associated Press, 18 Dec 1992, officials in South Korea decided to use the abacus to tabulate 24 million votes in Friday's presidential elections. The abacus was used to avoid a recurrence of charges in the 1987 presidential race that the computer count was electronically manipulated. The Central Election Management Committee employed about 300 abacus experts to oversee the counting.

It's curious that these people find manual manipuation -- an unnecessary backformation, since manipulation *means* movement by hand -- of an election to be preferable to electronic manipulation. [A Deutsche Press-Agentur news item quoted a Committee official who said, ''We are sorry we can't use the fast and economical way of tallying with computers but we like to be fair and accurate above all.'' PGN]

Systems causing unintended changes in behaviour [Bell Canada, Toronto Police] (From Doug Moore)

A couple of items in RISKS touched upon computer systems and technology affecting people's behaviour and causing changes in our society. There is a risk that some changes may be undesirable and unintended.

- Sometimes the change comes about because a system lacks sufficient information and or isn't smart enough to handle it. When working at Bell Canada back in the '70s, I saw an example of that. A system was supposed to compare numbers of long distance operators working with the number required to handle the load of calls. Over the long term it was hoped the information would help in predicting staffing requirements based on various factors. However, it was also used to evaluate managers on their current success or lack of success in matching the number working with the number needed. One serious flaw was that the program assumed the actual number of operators working could be changed every half hour. This assumption was at odds with the union contract that put minimums on the number of hours in a shift and limits on scheduling of shifts. The result was that at the end of each day managers would spend time doing nothing but telling operators to unplug or plug into the system in an attempt to fool it. Manager and operator behavior was changed in a way the company hadn't intended.

- Sometimes a change comes about simply because it is easier for a system to deal with data where quantities or levels are significant compared to other data, and managers may place too much emphasis on that data.

- The Metro Toronto Police may have changed their system by now, but at one time, their system reported statistics each week on the activities of each police officer - just in order to ensure sound management of staff resources, of course. Such things like numbers of parking tickets issued were easy to input and report. A wide variety of other activities, such as taking a lost child home, or spending some time checking into a broken window at a business, could not be as easily input or reported in meaningful ways, yet the value of those other activities may be far more. Supervisory officers would, of course, recognize the value of such activities in principle, but the common reaction to the weekly report was to notice such things as few parking tickets being issued, to require explanations when that happened, and to tell the officers to spend more time on issuing parking tickets so that next week's report wouldn't ''look so bad.'' The net result of such a system changes the police officers' behaviour. While they would be unlikely to ignore other matters that came up, the officers would nonetheless concentrate on the activities that easily produced large numbers on the reports - such as issuing parking tickets.

In both of these examples changes happened that were not intended by anyone. How to predict and avoid or manage such changes may not be simple when a system is being designed or managed, but an effort is needed.

Library loses its card catalog (From Patrick White)

Here's a computer related risk I didn't expect to run into at my local public library...

Over the last few years, the public library system has been converting the card catalog and checkout system over to a (remote) centralized computer that provides all sorts of nifty features like dial in access, ability to check if a book is checked out, requesting books from other libraries and much more. Well, in the last year or so, they found that the paper card catalog was not being kept up to date, so, since they had the computer, they got rid of it. [Recently], a transformer blew and the computer went down (since it had no UPS, it went down hard and recovery included fixing hardware as well as restoring data). While the computer was down, it was still possible to check out books (apparently they had some sort of backup procedure in place for that), but there was no card catalog -- one had to ask at the reference desk to get a list of places to go look around in the stacks for books on their topic.

I talked with one of their computer services people and was told that they plan to put in a UPS for next time so the machine can be taken down safely and the data preserved, but there are no plans for anything beyond that (in particular, no decentralization was planned). Obviously, another blown transformer or other power/phone outage (we are expecting an unusually nasty winter) could take out the card catalog again. This certainly isn't a life-threatening sort of risk, but does illustrate one risk of computerizing an index at a site distant from the records.

Dutch chemical plant explodes due to typing error (Meine van der Meulen; earlier report from Ralph Moonen)

At a chemical factory a heavy explosion occurred which caused the death of 3 firemen of the works fire brigade and injured 11 workers including 4 firemen of the works fire brigade. The damage was estimated at several 10s of millions NL guilders. There was severe material damage. The fragments where found at a distance of 1 km. The accident started with a typing error in a recipe made by a laboratory worker. Instead of tank 632 he typed tank 634. In tank 632 there was stored resin feed classic (UN-1268) normally used in the batch process. In tank 634 DCDP (dicyclopentadiene) was stored. The operator, employed for three months and still in training, forgot to check if the tank contents were consistent with the recipe. Subsequently he filled the reactor with the wrong chemicals. The batch process started with steam heating via the coil in the reactor. After the temperature began to rise, first the operator tried to cool the reactor with more water from the water mains; later the works fire brigade was alarmed to cool the reactor.

An administrator, who checked the recipe every morning, found the error and tried to contact the operator, but it was too late. Because the works fire brigade expected that the contents of the reactor would be released via the safety valve and the bursting disc, they were connecting deluge guns to prevent spreading of the expected fire. The firemen did not wear the prescribed personal safety articles, such as hand gloves and breathing apparatus, because they expected to do a relatively easy job. After releasing chemicals via the safety valve and the bursting disc, several seconds later the reactor ruptured, the contents of the reactor released and an explosion followed. The local fire brigade was alerted and together with the works fire brigade, they tried to prevent the fire from spreading to the other installations, such as cylinders filled with boron trifluoride. To prevent enormous damage to the environment due to polluted fire fighting water, it was decided to let the fire burn out by itself. In court, the judge ruled that the management of the company had had insufficient attention for safety and the company was fined 220,000 NL Guilders. [Source: ''FACTS, Database for Industrial Safety Acc.#: 11057, Extended abstract'', NL, 1992 Jul 08. This information is compiled by TNO with greatest care from qualified source documents. TNO cannot accept responsibility for any inaccuracy. Piet van Beek, The Netherlands Organization for Applied Scientific Research TNO, Department of Industrial Safety, Apeldoorn, The Netherlands, Phone: +31 55 493810, Fax: +31 55 493390] [PvB via MvdM]

Risk Management (From Phil Agre)

Both of the following books are deeply concerned with the social management of risk, technological and otherwise.

• Brian Wynne, *Risk Management and Hazardous Waste: Implementation and the Dialectics of Credibility*, Springer-Verlag, Berlin, 1987. This book is the report of a project at the IIASA in Vienna on the politics of regulation of hazardous wastes. This is a fascinating enough topic on its own, but what's particularly relevant about this particular study is its attention to the administrative dimensions of regulation and risk. Wynne et al. spell out in a sophisticated and sustained way an argument already made by Charles Perrow and others, that risks are located not exactly in technologies but in the institutions (and by extension the larger cultures and social arrangements) that contain them. This view has many consequences (at least, several more than I had thought about myself), which Wynne explains with some force.

• Lorraine Daston, *Classical Probability in the Enlightenment*, Princeton University Press, 1988. This is a detailed and scholarly history of early modern mathematical ideas of probability. Though not really a social history, it focuses on the developing practices of life insurance, lotteries, and gambling, tracing the shifting ideas about the morality and rationality of these things. It was not until the early 19th century, for example, that insurance ceased to be understood as a variety of gambling. And Daston explores at length various explanations for the great slowness with which insurance companies came to use probabilistic models rather than individual interviews and judgements.

Her central argument, though, concerns the rise of the idea of large-scale statistical regularities. She says: ''Whereas De Moivre took the order revealed in stable statistical frequencies as incontrovertible evidence that an intelligent agent was at work in the world, Poisson argued that such order was only to be expected; we should suspect divine tinkering only when it was absent. For the mathematicians, the clock no longer implied a clockmaker. The ascent of statistical regularities ultimately marked the decline of the reasonable man, as probability theory shifted its sights from the psychology of the rational individual to the sociology of the irrational masses (page 187).'' ''Consequently, the targets of persuasion also differed: Quetelet wanted governments to change their ways on the basis of his figures, not individuals. But both sorts of probabilistic rationality presupposed the stable, orderly phenomena that made calculation possible, even if they singled out different *kinds* of phenomena as quantifiable. Classical probabilists believed that judicial decisions, but not traffic accidents, were regular; their successors believed just the reverse (page 385).''

(From Gary McClelland)

I second the recommendation for reading Daston's histories. For those with limited time, I recommend as a shorter course this chapter: Daston, L. J. The domestication of risk: Mathematical probability and insurance 1650-1830. In L. Kruger, L. J. Daston, & M. Heidelberger (Eds.), The probabilistic revolution: Volume 1. Ideas in history (pp. 237-260). Cambridge, MA: MIT Press, 1987.

It is interesting to look back and see the probabilists scratching their heads trying to understand the boneheadedness of both users and designers of insurance systems (e.g., the Bank of England almost went broke by selling lifetime annuities at a fixed price *not* conditional on age). I think readers of RISKS often scratch their heads in the same way trying to understand the boneheadedness of both users and designers of computer systems. The good news is that the insurance companies finally got it right with respect to probability. The bad news is that it took a long time and required some fundamental shifts in thinking about probability and uncertainty. RISKS readers may therefore find some lessons in Daston's work on what must occur before designers and users of computing systems (ironically, of course, the insurance companies are now big users) more appropriately deal with the risks of computing. Alas, the Bank of England was near bankruptcy before they wised up, so the message may not be comforting.

Overheard by Don Knuth on a recent trip (From Phyllis Winkler via Les Earnest)

Q. What kind of computer music will President Clinton play on his saxophone?

A. Al Gore rhythms. [From the Cornell U Linguistics Department]

Under 50 miles hurts with Hertz [Hertz hat kein Herz?] (From Bruce N. Baker)

Hertz Rent-A-Car has recently implemented an advanced fuel purchase option. The option permits drivers to pay for gas at the average self service price in the area of the car rental. The option only benefits those drivers who use more than a full tank of gas. Otherwise, you must show your gas receipts upon returning the car, if you claim that you are returning the car with a full tank.

An interesting quirk of this system is the programming of the portable check-in palm-top computers used by the attendants who wander along the lanes where you return your car. If you have driven less than 50 miles, the system is programmed to automatically charge you $5.00 for gas, even if you have a receipt showing that you have filled it up. Hmmm... let's see... if the average distance driven by those who have driven less than 50 miles is about 35 miles, that equates to about one gallon of gas for the $5.00 charge (vs. about $1.15 at the tank). Are Ross Perot's gas prices already here? To override the check-out slips provided by the attendants from their palm-tops, you have to take your receipt into the main check-in area. If you're in a hurry, chances are you won't. Then Hertz has the full tank of gas *and* your $5.00. Luckily, my attendant informed me of this quirk. Chalk up another one for American ingenuity!

Florida Rental Car Scam (From Dewey Coffman)

Ex-Car Rental Owners Indicted, FORT LAUDERDALE, Fla. (AP, 10 Jan 93) Value Rent-A-Car Inc. rigged its computer system to set up a scam overcharging customers who returned their cars with less than a full tank, a federal indictment says. The indictment returned Friday says Steven M. Cohen, one of three former owners charged, fixed Value's computer system in 1988 to add five gallons to the fuel tank capacity of every vehicle in Value's fleet. This allowed the company to overcharge customers who turned in the car with less than a full tank. Federal prosecutor Lothar Genge said that through 1991, about 47,000 customers were slapped with the phony charge, which ranged from a couple of dollars to $10 or $15. Mitsubishi Motor Sales bought the company in 1990 and is looking for ways to pay back the overcharges, Genge said.

Student Loan Errors Blamed on Computer (From Steve Peterson)

Because of a computer problem, thousands of college students have been sent notices ordering them to begin repaying loans that aren't due, a loan-processing company in St. Paul [Minnesota] says. Shirley Chase, an attorney for EduServ Technologies, ... said problems with a new computer system caused a backlog in processing student requests to defer payments. She said the company hopes to clear up the backlog by the end of February. More than 10,000 deferment forms are backlogged, she said. Because of the backlog, some students who are entitled to postpone their loan payments have gotten notices urging them to pay and some have been contacted by a collection agency. Chase said EduServ has "bent over backward" to make sure no adverse credit reports are filed with credit bureaus because of the delay. EduServ processes loans issued by banks and other lenders and make sure payments are current. [AP, Minneapolis Star Tribune, 12 Jan 1992]

Comment: Given that they probably had a choice of whether to send dunning notices to everyone or temporarily stop sending them, it shouldn't be surprising which choice they made.

[PGN's daughter Hellie reported in from Massachusetts that she had seen a message displayed in front of PJ Auto Sales in Swampscott MA, bearing on an old RISKS theme, worthy of note here:

TO ERR IS HUMAN. TO BLAME IT ON A COMPUTER IS EVEN MORE.]

Air Inter politics (Peter B. Ladkin)

COLMAR, France (AP) - A former official of the French domestic airline Air Inter was charged Monday with negligent homicide in the crash of a passenger jet a year ago that killed 87 people. Jacques Rantet, Air Inter's former director of flight security, was charged ... with negligence leading to death and injury in the crash of the Airbus A320. Nine people survived after the airliner crashed into a mountainside as it approached Strasbourg airport on Jan. 20, 1992. [Paris charges ex-official in air crash, International Herald Tribune, 19 Jan 1993]

London Ambulance Service (From Brian.Randell)

[Brian reported on a front page story in the (UK) Computer Weekly, 18 Feb, 1993.] The article leads with a report that the chairman of the London Ambulance Service, Jim Harris has resigned. The article repeats the union claim that up to 20 deaths resulted from ambulance delays, but states that this allegation is hotly denied by management, adding that: ''Yesterday's document shies away from linking deaths directly with ambulance delays caused by the computer crash. It said an examination of 26 cases at coroners courts since November 1991 showed that the LAS had not been blamed for a single death. Two cases are outstanding.''

On 26 Feb 1993 the UK national newspaper The Independent covered the just-released report very fully -- it was the main story on the front page (entitled ''Report Prompts Departure of Ambulance Boss''), with three more stories taking up a significant fraction of page 3. These are entitled ''Managers 'created an atmosphere of mistrust' '', ''[Secretary of State for Health] Bottomley condemns 'catalogue of errors' '', and ''Father grieved for asthmatic son who died in his arms.'' The first of these, by Susan Watts, had the following statement:

> It would be hard to paint a more damning picture of failed management than that which emerged from the inquiry into the London Ambulance Service yesterday. The report said that the LAS management ''created an atmosphere of mistrust'' with its over-aggressive style, born in part out of the desperation to put right decades of poor performance.
>
> The LAS made ''virtually every mistake in the book'' when implementing its 'ambitious' 1.5-million-pound computer system, one of the three-strong inquiry team said. The computer-aided dispatch (CAD) system was seen as the only hope the service had to put right its poor response times in dealing with emergency calls. But the software was ''not complete, not properly tuned, and not fully tested.'' the report said. The inquiry team was set up after the CAD system broke down on 26 and 27 October last year, then collapsed a second time on 4 November, forcing controllers to revert to pen and paper to dispatch ambulances.

Miscarriages -- chip workers in the U.S., VDT users in Finland

The four-year study by the University of California at Davis reports that women making computer chip's have a 40% higher incidence of miscarriages than other workers in the same factories. It covered 15,000 workers at 14 factories in seven states. A previous study by the University of Massachusetts reported a 70% increased risk among women in a particular factory of Digital Equipment Corp. [Source: San Francisco Chronicle, 4 December 1992, p.1.]

Researchers in Finland have identified a statistically significant incidence of miscarriages among women using computer video display terminals that emit electromagnetic radiation of type ELF -- triple the expected normal. A report is being published in the American Journal of Epidemiology. [Source: San Francisco Chronicle, 10 December 1992, p.A7]

Incidentally, Paul Brodeur has another article on electromagnetic radiation effects in the New Yorker dated 7 December 1992. [RISKS readers will recall the previous series of three articles being discussed here, e.g., ***SEN*** 15, 5, October 1990. Forewarned is not necessarily forearmed, even if you have four arms. But this problem really demands greater attention, even if there are some who say these studies are not definitive. PGN]

Computer games may endanger your health

Nintendo Inquiry Launched -- The Government is probing claims of health hazards to children playing computer games like Nintendo. The informal inquiry follows reports that two boys in Cardiff had been struck down with epileptic fits. Baroness Denton, junior Consumer Affairs Minister, has called for an urgent report: 'It is important to know if there are any health risks. [From Teletext service on Carlton TV & Channel 4 (UK), 7 Jan 1993, noted by Olivier M.J. Crepin-Leblond]

[The Nintendo Entertainment System Manual notes that people with a history of epilepsy may experience seizures, and admonishes thusly: ''Consult your physician if you experience any of the following symptoms while playing video games: altered vision, muscle twitching, other involuntary movements, loss of awareness of your surroundings, mental confusion, and/or convulsions. (Reported in RISKS by Rick Russell). J. Eric Townsend noted that there were similar problems with the Commodore 64. PGN]

'Untested' Risk Management System for Nuclear Power Stations (From Anthony Naggs)

Sacked expert fears nuclear safety risk (Paul Brown, Environment Correspondent, The Guardian, 4 March 1993)

A computer system created to make Britain's nuclear reactors safer could fail at a vital moment because it has not been tested properly, according to the man who designed it. Bob Hodson-Smith, who has been sacked by a company commissioned by Nuclear Electric to design a back-up safety system for nuclear power station controllers, says the system might not perform adequately at precisely the moment it was needed because 'bugs' had not been removed from the programming. He has expressed his fears to Nuclear Electric, the state owned company that runs [all commercial] nuclear power stations in England and Wales. It is understood that the company is seriously concerned at the implications. The firm that sacked him, Active Business Services (ABS), of Sheffield, has described his fears as irrational. But Mr Hodson-Smith says: ''I could no longer live with the fact that safety might be compromised and I had done nothing to warn anyone.''

SUBSECTION ON BANKING SYSTEM RELIABILITY

Leap year causes problems for ATM machines (From Conrad Bullock, excerpted by PGN)

Beginning at midnight on 31 December 1992, several thousand ASB regional bank customers had their transactions rejected, due to a ''faulty date checking routine'' that could not handle the end of the leap year properly. The problem was fixed by 10am. All of the customers who used the system in that period had their bank-card magnetic stripes corrupted. Transactions were rejected only for those who tried to make a second transaction. (''Year too long for money machines'', By Roger Fea, New Zealand Herald, 2 Jan 1993) The same phenomenon also was reported for 1500 TSB regional bank customers in Taranaki, from midnight until after noon. (''Leap year spikes cashcards'', NZPA, Waikato Times, 2 Jan 1993.) Both banks use an NCR ATM system. This was another example of the new day hitting first in New Zealand, which is proving to be the king's taster for clock problems. (The Tandem CLX system broke at 3pm on 1 Nov 1992, reported in our previous issue.) PGN excerpting.

Resolution Trust Corp overreports interest paid (From Jeremy Epstein)

According to a Washington Post article [during the last week of Feb 1993], the Resolution Trust Corporation [the federal agency charged with cleaning up failed savings & loans] generated incorrect data on Form 1099s [that's the form that tells the Internal Revenue Service how much interest you earned for the year, so you pay tax on it]. According to the article, there have been some serious glitches, including a woman whose 1099 reported $152,000 in interest, rather than the $3,000 she actually earned. Other statements were off by a factor of 100 or more. According to the article, the IRS was not sent the erroneous figure, although about 2000 customers of the failed Trustbank received incorrect notices. The error occurred because ''of a computer tape mishap'' according to an RTC spokesman. No further details on the mishap were provided.

As more and more data is submitted to the IRS electronically, and the IRS does more and more electronic cross-checking, it's easy to see how people could have received automatic dunning notices for underreporting their income, had the erroneous data been sent to the IRS. I wonder whether the IRS's analysis software (or auditors) would have noticed that for many people, the amount of interest reported was highly unlikely given their historical tax data and income.

Citibank outage (From Marty Leisner)

Software Problem Halts Citibank's Automatic Tellers for 4 Hours (Sunday NY Times, p.43, Metro, 14 Feb 1993)

Citibank's 1200 ATMs went down (refused to dispense cash or complete transactions) from 10AM to 2 PM on Saturday because of ''a software glitch'' when new software was being installed.

Esperanto from a computer error (From Philip Brewer)

The following appeared in the November 1992 issue of *Esperanto*, the publication of the Universal Esperanto Association. (This is my translation from the original Esperanto.)

> Portugal: Esperanto from a computer error
>
> Hans Jankowski (German) was pleasantly surprised when a money-changing machine from the Totta and Acores bank in the Lisbon airport gave him his receipt in Esperanto. Because the Portuguese Esperanto Association was also surprised, Antonio Martins decided to explore. It seems that this was probably an error in setting up the computer: on installation of the ten-language system, someone mistakenly programmed esp-eranto instead of the Spanish (esp-anol). So, no one should congratulate the bank; they plan to rectify the 'mistake'!

Their guess as to the origin of the situation certainly sounds plausible to me, although they apparently did not contact the bank to find out for sure.

''Bank Machine Glitch Leaves Users Poorer, But Empty-Handed'' (From Randal Schwartz)

Something like 18,000 west-coast U.S. Bank ATM transactions were stymied when users tried to withdraw money between 4 a.m. and 10:30 a.m. on 25 Feb 93; they received no cash, but the computer software in the U.S. Bank's Exchange system subtracted the money from their accounts anyway. Only users who were *not* U.S. Bank customers were affected. During that time, the bank was modifying its software at its main computer in Portland. [Source: The Oregonian, Sunday, 28 Feb 93, from staff and wire reports]

SUBSECTION ON TELEPHONE SYSTEM RELIABILITY

''Telephone Service Cut Off'' (From Lin Zucconi)

The Valley Times (18 Feb 1993) reported that telephone service was cut off for more than 4 hours to about 37,000 phone lines in Livermore, CA including '911' and operator 'O' lines. The article said that ''the significance (of the malfunction) was in having three prefixes that can't reach emergency phone lines... The phone company [Pacific Bell] was stymied in correcting the problem because diagnostic tests of the equipment told technicians that there was no problem... Technicians eventually located the problem in a call processor computer tape and replaced the malfunctioning tape.'' Luckily for those of us that live here, this is a relatively low crime area and no serious crimes occurred during the outage. Some banks compensated by letting in only a few customers at a time because they were concerned that their alarm systems wouldn't be able to call police.

''Computer Blamed For Phone Jam'' (From Joe Brownlee)

[From the Columbus (Ohio) *Dispatch*, by Ron Lietzke and Bruce Cadwallader, 28 Jan 1993]

> A three-minute computer failure at an Ohio Bell central office disrupted phone service for 42,000 telephone lines in the Downtown business district for about 45 minutes yesterday morning. The computer problem cleared after a few minutes, but the disruption snowballed when a surge of callers seeking dial tones caused a telephone traffic jam of sorts, Ohio Bell spokesman David Kandel said. Outgoing and incoming calls on 15 Downtown prefixes were disrupted by the problem, which started at 9:42 AM. The Columbus police, the Franklin County Sherrif's Department, Columbus Public Schools, and state offices were among those disrupted by the outage, Kandel said.
>
> Callers in the affected prefix areas who dialed 911 could not reach Columbus police or the Franklin County Sherrif's office for at least 3 minutes. However, those agencies reported that they did not receive any complaints after the dial tones returned. ''It was starting to clear itself within minutes, but because you're looking at such a huge volume of calls Downtown, it took the system time to recover,'' Kandel said. ''The system was delivering a very, very slow dial tone.'' Problems started when one of two computer processors failed. The other took over, but it took about three minutes for it to retrieve the information from the failed processor. Ohio Bell technicians were working with the equipment manufacturer yesterday to determine what caused the processor to fail.

I note two items of interest. One is that even a brief delay in grabbing data from the failed computer resulted in a large backlog. Perhaps the system was not designed to account for the large number of lines in downtown Columbus, which boomed during the 1980's. Phone systems tend to use less than state-of- the-art technology (to avoid many of the 'bleeding edge' problems often noted here), but in this case, perhaps a faster processor or live mirroring of the data in question would have helped.

As to my second point, twice the article points out that nobody knew of any emergency calls that were missed, with the implication that no harm was done. Dead men tell no tales?

More on Ohio phone problems (From Bill Warner)

One of the major causes of the long time to get the data from the failed computer is that phone switches have a lot more 'state' than they did in the past. For example, the State of Ohio Centrex (where I work in the telecom office) is served by the switch that failed [see above]. [The State of Ohio phones were dead for about 14 minutes or so. This likely affected the Franklin County Ohio Highway Patrol Post's (and General Head Quarters) public numbers also.]

We have somewhere over 20,000 lines (I don't keep up with the details.) In the past we had to configure options like Call Forward No Answer and Call Forward Busy with written service orders. But now each line has an option called Call Forward No Answer Universal (at least the name is close!), which allows someone at the phone to specify the number to Call Forward Busy to. This can be changed at any time. Therefore in the case of a switch failure you can not just return to the 'standard' configuration, but must load a lot of 'state' information from the failed computer. This type of state is becoming more common in 'fancier' features. It makes it much easier to manage a large number of phones! Features like call forwarding, which also require the switch to remember a number, are becoming more and more common.

- Blown Fuse Disrupts Phone Service (The Columbus Dispatch, 17 Feb 1993, p.3C, Metro)

A blown fuse in the Ohio Bell switch serving 54,768 telephone lines in Worthington disrupted service throughout the day yesterday. Repairs were expected to be completed last night. Ohio Bell Spokesman Keith Jameson said 911 and other emergency numbers remained in operation, although getting a dial tome within the affected area was slow. Calling into the area was difficult most of the day, since Ohio Bell purposely blocked 75 percent of incoming calls while repairs were under way. Jameson said that strategy enabled people within the area to make calls. By 5 PM, the company had reduced blocked incoming calls to 50 percent. The switch shut down at about 10:30 AM, when at least one fuse blew, but Jameson said there may be other problems with the switch. The problem was not weather related, he said.

Long Distance...is the next best thing to praying there (From Paul Robinson)

News of the Weird, by Chuck Shepard, *Washington City Paper* of 19-25 Feb 1993, p.18:

In January, Israel's national telephone company initiated a fax service that transmits messages to God via the Wailing Wall in Jerusalem. In May, the Roman Catholic Church will unveil a high-tech confessional at a trade show in Vincenza, Italy, that will accept confessions by fax. And in December, a sect of Orthodox Jews in Brooklyn, NY began selling its members special beepers so they will know instantly when the Messiah arrives.

Computer delays response to fatal fire (From Lauren Wiener)

A 'computer error' was blamed for a 7-minute delay in a response to an emergency 911 call, allegedly because an address (12229 Hillar Road) was consistently being transformed (into 1229), which resulted in the call automatically being redirected to the wrong dispatch office. One person died, and presumably could have been saved but for the delay. The telephone company later discovered that a system reload had been done that caused the misdirection, which would also have affected other people in Multnomah County who were served by an outside fire agency. [Source: Computer delays response to fatal Bonny Slope fire, by James Mayer, From the Oregonian, Saturday, Feb. 20, 1993, p.B1; abridged by PGN]

911 in Massachussetts (From Barry Shein)

[Barry Shein reported on a Boston woman who was murdered by a man (her ex-husband?) whom she heard at her door. She had called 911, but because her exchange was a Brookline exchange, not properly a part of Boston, the call went to the Brookline police -- who informed her she needed to call the Boston police. PGN].

Doctor service phone logs skewed (From Steen Hansen)

A new central system is being tested in Denmark for people to call a doctor service at off hours, and possibly get a housecall (this is for non-emergency cases, i.e., not the equivalent of 911). The patients in the Danish city of Odense complained loudly that waiting for the phone call to be answered was too long, whereas the provider said their computerized logs showed no caller had to wait more than 10 minutes. After many complaints they tested the equipment, which showed it was not able to register waits longer than 10 minutes.

Phone company writes a letter to a public telephone (Warren Burstein, via Mark Brader)

warren@itexjct.jct.ac.il writes in comp.dcom.telecom:

> Yerushalaim (a Jerusalem local newspaper) [14 August 1992] contains a copy of a letter that Bezeq, the Israeli telco, mailed to a phone booth which it owns. The form letter is addressed to 'Bezeq, Inc.' at the address at which the phone booth is located (155 Costa Rica Street), and informs the subscriber that while in the past, its bill was computed by reading a meter, which made it impossible to obtain a listing of calls made, this will now be possible (at a fee, of course, something that Bezeq did not mention to the phone booth). The letter-carrier delivered the letter by placing it inside the phone booth. Bezeq responded that the program that sends out mailings will be corrected. The phone booth was unavailable for comment.

SUBSECTION ON SECURITY AND PRIVACY

Cable freeloaders (From Tony Scandora)

Continental Cablevision of Hartford broadcast a special offer of a free T-shirt during the Holyfield/Bowe fight on 14 Nov 92. Unlike most pay-per-view broadcasting, this one did not show up through legitimate decoders. The ad and its 800 number only showed up when watched through illegal decoders. 140 freeloaders called the 800 number within minutes of the ad's broadcast. Continental sent the T-shirts by certified, return receipt mail, and then sent them a followup letter reminding them of the federal law (fines up to $10,000) and demanding a $2000 fine. [Chicago Tribune, 3 Feb 1993]

Antipiracy tactics: "Computer Cheats Take Cadsoft's Bait" (Jay Rolls via Gio Wiederhold)

Employees of IBM, Philips, the German federal interior ministry and the federal office for the protection of the constitution are among those who unwittingly 'turned themselves in' when a German computer software company resorted to an undercover strategy to find out who was using illegal copies of one of its programs. Hundreds of customers accepted Cadsoft's offer of a free demonstration program that, unknown to them, searched their computer hard disks for illegal copies. Where the search was successful, a message appeared on the monitor screen inviting the customer to print out and return a voucher for a free handbook of the latest version of the program. However, instead of a handbook the users received a letter from the Bavarian-based software company's lawyers. Since the demonstration program was distributed last June, about 400 people returned the voucher, which contained coded information about the type of computer and the version of the illegally copied Cadsoft program being used. Cadsoft is now seeking damages of at least DM6,000 (ECU3E2) each from the illegal users.

Cadsoft's tactics are justified by manager Rudolf Hofer as a necessary defence against pirate copying. The company had experienced a 30% drop since 1991 in sales of its successful Eagle design program, which retails at DM2,998. In contrast, demand for a DM25 demo version, which Cadsoft offered with the handbook of the full version, had jumped, indicating that people were acquiring the program from other sources. Although Cadsoft devised its plan with the help of lawyers, doubts have been raised about the legal acceptability of this type of computer detective work. In the case of government offices there is concern about data protection and official secrets. The search program may also have had side-effects that caused other files to be damaged or lost. Cadsoft is therefore preparing itself for what could be a long legal battle with some customers. So far it has reached out-of-court agreement with only about a quarter of those who incriminated themselves. [Jay Rolls, Stuttgart, Germany; appeared in info-mac]

Two Charged with Computer Fraud in Credit Scam (From Norm deCarteret)

St. Petersburg Times, 26 Jan 93, pg 3B, by Tim Roche

A personnel supervisor "who knew the ins and outs of a computer system that managed charge accounts for thousands of jewelry store customers along the Eastern Seaboard" and a former co-worker worked a scam using the supervisors' ability to alter the computer's database, illustrating the risks of:

- inadequate controls within the computer system
- retail store policy shortcomings
- the procedure by which they let users who have had their card stolen continue to charge purchases
- flaws in the system accountability

Using computer passwords of other employees, detectives said, Benjamin Francois was able to alter customer records and list a credit card as lost or stolen. Then his friend, John Wise, would appear at a jewelry store and claim to be the customer whose credit card was missing. By store policy, Wise was required only to give sales clerks a name, Social Security number and a secret code that would allow customers whose cards were lost or stolen to continue charging merchandise. "If the clerk asked to see some identification, Wise would explain ... he had no photo to prove he was the customer, but he would give the clerk the secret code Francois had obtained from the computer." Affected between June and September 1993 were jewelry stores in Tampa, Orlando, Palm Beach and Altamonte Springs FL, and Jewelers Financial Services, which ran accounts for Zales Jewelers, Bailey Banks & Biddle Jewelers, Gordons Jewelers. Francois was able to delete the references to stolen or lost cards on the charge accounts after the purchases were made. The two men were arrested after a tip in November led police investigators to "verify the mainframe database" records. Of particular interest: system controls allow Francois to manipulate the database, then hide the activity so that, apparently, the real customers were not billed. If the report is correct, it was the November tip and not any system controls that revealed the thefts. Apparently the charges were allowed to fall into some sort of accounting black hole.

Ross Perot Campaign Steals Credit Data? (From Richard N Kitchen)

News reports indicated that the Ross Perot campaign is being investigated by the FBI, Secret Service, and Federal Trade Commission for allegedly using stolen computer codes to obtain credit reports on some campaign workers. Investigators refused to discuss the case, but former Perot campaign employees, Equifax (the credit reporting company) and Orix Consumer Leasing of Secaucus, NJ admitted having spoken to investigators. Equifax said at least seventeen credit files of former Perot campaign workers may have been accessed illegally. Some Equifax reports were obtained using the security code of Orix, which claims to never have requested the credit reports on Perot volunteers. Officials at Orix and Equifax have said they believe Orix's security codes were stolen. [Source: LA Times 2 or 3 Jan 93]

Public Service for Cornell Hackers (From D.C. Lawson)

Public Service for Hackers, by John Marcham, *Cornell Alumni News* magazine (Jan 1993?)

Two former [Cornell] students will develop a computer program to make it easier for a quadriplegic man in Tennessee to use a computer he owns, as part of their punishment for launching a computer virus that damaged programs and caused hard drive crashes last February. David Blumenthal '96 and Mark A. Pilgrim '94 were sentenced by a Tompkins County Court judge to pay restitution to users whose computers were jammed by the men's virus, at and near Stanford University and in Japan, and to perform ten hours of community service per week for a year. A computer buff who knew the quadriplegic and heard of the Cornell virus case wrote the judge in Ithaca, and asked if the students' public service could be worked off developing a less expensive and cumbersome program for the disabled man, who uses a mouthstick and outdated software to operate his McIntosh computer. The judge and the former students agreed to the proposal: the students start work in November. A third former student, found guilty of a lesser infraction, was asked but not required to do public service, and declined.

Brazilian Banking Reserve Data Disappears: The Post-Hacker Era (From Sanford Sherizen)

A Reuters report found in the NY Times (21 Jan 1993) states that computer disks holding secret information on Brazil's banking reserves have disappeared from the central bank. The federal police are investigating the loss. According to the report, President Itamar Franco "took the unusual step" of releasing information on the reserves to offset any damage or financial speculation from loss of the disks. The disks held information on day-to-day reserve operations and details like where the reserves are invested, what they consisted of and how the reserves were generated.

Comments: This disappearance may be related to ex-President Collar's involvement in the looting of Brazil. At a minimum, the data disappearance seems to be another indication of the Post-Hacker Era, where governments and companies have learned that computers can be used as an essential aspect of crime and/or to cover up a crime. The lines between 'hacker' activities and 'legitimate' activities may become increasingly less clear. In order to commit a white collar or economic crime, individuals or organizations will almost have to use computer techniques. While there continues to be an (often unconscious) image that many have that computer crime is 'bad individuals' against 'good' organizations, the Organization as Computer Criminal is rapidly becoming a serious problem. One but certainly not the only instance of this is the recent British Airways's penetration of Virgin Air's reservations system. [Added note: One British tabloid had the headline, *Virgin Screws BA*, which apparently seemed more newsworthy than the other way around.]

Computer hacking of flight details 'was illegal' (From Jonathan Bowen)

The 12 Jan 1993 UK newspapers are full of the story on the British Airways (BA) 'dirty tricks' campaign against Virgin Air and their successful suing by Richard Branson. Of particular relevance to RISKS is the following extract from *The Independent* (12 January 1993, p6): "The [BA] team were told that in future, their key task would be to access highly confidential information from their rival's [Virgin's] computer system. "We were shown how to get the information by tapping into our computer terminals in the Helpline office. We tapped in with our regular BA code and called up the Virgin flight numbers." In common with many other airlines, Virgin rents out a segment of a vast computer known as Babs - British Airways Booking System. Mr Khalifa and his colleagues simply tapped into it. "We could see on the Babs computer system when flight is open [sic], when it closed, if it was delayed and how many passengers were due to board.'' For the next nine months the Helpline hackers provided BA with critical information on Virgin's flights."

Toronto Stock Exchange Virus Scare (From Shyamal Jajodia)

Information Week reported that someone described as a disgruntled former employee of the Toronto Stock Exchange telephoned a local TV station newsroom and claimed that he had placed a computer virus in the exchange computer system due to activate at 9:30 the following morning. An all-night search of the system did not reveal any infection, and trading proceeded on the following trading day without interruption. This risk is similar to the risk of bomb scares on flights. Seems that all systems vulnerable to threats that cannot be detected without considerable work are vulnerable to the risk of false alarms. [Source: EDPACS Newsletter, Jan 1993]

Computer Theft of Criminal Records (From Gary McClelland)

A private investigator and two police employees have been indicted by a Denver grand jury for improperly obtaining the criminal histories of 8,559 individuals. The private eye paid $3 to $5 per search and as much as $1,300 per week (he kept great records!). The scheme unraveled when a co-worker of the police employee who was doing the snooping became angry that her colleague was spending so much time looking up names that she was falling behind in her regular work. So after seeing a 'criminal history format' on her screen that she was not supposed to be using, the co-worker turned her in. A computer log revealed that on the day she was caught, she had run checks on 95 people! It turns out that a transaction recording system allowed investigators to reconstruct all 8559 criminal history searches. With such a great logging system, it seems strange that no one noticed 8559 extra searches; if the co-worker hadn't had the extra work dumped on her, these folks would still be stealing criminal records. [Source: AP, Boulder Daily Camera (8 Jan 1993), reporting a familiar story with a few new variations.]

KIO diskettes stolen from the Spanish Government (From Miguel Gallardo)

During the night of 5 February 1993, 18 diskettes were stolen from the Ministry of Economy and Taxes in Madrid, Spain. All the diskettes contained information of international funds transferred by Kuwait Investment Office (KIO) since 1988. The situation of this large group of chemical, building and real estate companies in Spain is very complex, because many of them are in bankruptcy, the Spanish Government has paid a lot of money to support this industry, there are thousands of people losing their jobs, present managers of KIO in Spain demanded old jobs at the Court, and there is evidence of money fraud and political corruption.

Javier De la Rosa, Fouad K. Jaffar and Mohamed al Sabah are the names most often mentioned in several press items that compare their management with Michael Milken (convicted), John H. Gutfreund, Donald M. Feurstein (Salomon Inc) and other Securities & Exchange Commission affairs in USA. But they control many journalists here, thanks to the singer Julio Iglesias' ex-manager, and now Javier De la Rosa's speaker [spokesman?], Alfredo Fraile. The Government Minister, Carlos Solchaga, told the press that he thinks the goal of the thief is to sell this information to the press, and to discredit *him*. He advised journalists not to buy this interesting digital information, because legal prosecution will be ordered if anything is published. On the other side, Javier De la Rosa told the journalists that there is a mafia in Spanish bureaucracy that stole the diskettes. But this is not a clever idea because it is not necessary to steal something that can be easily diskcopied.

What is much more interesting is that KIO has nothing to say, and that a Spanish Justice refused to accept its demand because there was not enough information enclosed. It seems that they did not find a computer expert capable enough to look for financial scandal data in computers and back-ups, now owned by them. IMHO, everybody has too many things to hide in this sad story.

Japanese Bank Hit By Phone Fraud (From John Mello)

A Boston branch of the Daiwa Bank Ltd., the 25th largest bank in the world, was victimized by prison inmates with a gift for social engineering, according to the Boston Business Journal. The inmates placed collect calls to the Daiwa switchboard, identified themselves as telephone repairmen, and said they could fix the company's telephone problems by being connected to an outside line. Once connected to an outside line, the cons made long-distance calls, sticking Daiwa with the tab. Some of the calls were to sex hotlines.

Hospitals in the Boston area were some of the first victims of this form of phone fraud, the newspaper reported. Inmates treated at the hospitals would memorize employees' names or use the names of physician's who appeared on TV to con operators into giving inmates access to outside lines. Once the operators got wind of what was happening, though, the hospitals were able to clamp down on the problem. One inmate,`impersonating a doctor who appeared on TV the previous day, gave himself away by referring to himself by title 'doctor'. The operator knew the physician always identified himself by his first name. the last thing the jailbird heard before the operator hung up on him was, "I suggest you speak to the warden about that." [The Boston Business Journal, Feb 1993]

Hacker disables cancer database (From Jonathan Bowen)

A schoolboy computer hacker caused chaos when he dialed into a vital database at a Brussels-based centre for cancer research and treatment. Paul Bedworth allegedly ran a rogue program that generated 50,000 phone calls, and caused the computer system at the European Organisation for the Research and Treatment of Cancer to 'crash'. In the process, Mr. Bedworth, now 19 and a student of artificial intelligence at Edinburgh university, left the centre with a 10,000 pound [c. US$14,000] phone bill. His trial is in progress. [Abridgement by JB and PGN of an article in the Home News section (page 4) of the Guardian, UK, 25 Feb 1993] Reuters (noted by Mich Kabay) says Bedworth also broke into the British Telecom telephone network, a Lloyds Bank computer, and the Financial Times of London. PGN]

And you thought your computer chat was private! (From Marty Leisner)

In the 7 February 1993 NY Times, p.32, was an article detailing privacy issues with email. They talked about Oliver North's message in 1986 to his aide Ronald Sable: "Oh Lord, I lost the slip and broke one of the high heels. Forgive please.. Will return the wig Monday." The article quotes Paul Saffo (Institute for the Future) talking about "we have yet to establish the conventions for e-mail."

Evacuation plan, generators fail in World Trade Center blast (From Jay Elinsky)

The New York Times, in its morning-after coverage 27 Feb 1993 of the huge explosion in the World Trade Center garage in downtown Manhattan, reported that the blast destroyed the complex's operations center and severed cooling lines for the emergency generators. The result was that there was no organized leadership in evacuating 50,000 people down the stairwells of the 110-story twin towers, and the ventilation system was unable to suck out smoke. [The toll was six killed (one missing person's body was discovered, three weeks later) and over 1,000 injured. PGN] The former director of the agency that runs the center said that studies in the mid-80's showed it could withstand a car bomb. " 'They said you could sustain a car bomb', he said. 'What they didn't tell us was you couldn't sustain it if it was perfectly placed.' "

[Added note: Maybe my submission was a bit hasty. The NY Times on 1 Mar 1993 says that the Port Authority *did* know in 1985 that a car bomb could disable building systems, but they decided not to implement the recommended changes because of the expense. JE]

Permanent records (Anonymous to protect privacy, forwarded by Richard A. Schumacher)

Some weeks ago, conversation on AFU turned to the existence of 'permanent records' for grade school and high school students. It turns out that the state of Ohio has been keeping computerized records of Ohio primary and secondary students. I quote from the *Columbus Dispatch*

> Virtually all school districts are sending 93 categories of information about each of Ohio's 1.8 million primary and secondary school students to 25 regional data centers. The information is linked to a student identification number, which the state says should be the student's social security number. The computer data include test scores, disciplinary action, medical details including pregnancy, race, handicaps and family income. [...]
>
> Princeton [a Cincinnati HS] supplies the state with statistics that do not identify students, [and] has never given information linked to names or identification numbers. As a result, the state has threatened to cut off the district's funding, beginning with its April payment of about $288,000. Princeton and other schools are suing the state based on the Federal Privacy Act. [...] Many districts don't even tell parents or students they are sending information about students to the state. [...]

Ohio has also kept a database of accusations of child abuse with 200,000 names on it. Ohio's population is about 11,000,000. It was, until recently, impossible to find out if you were on the list, and who accused you, and impossible to get your name removed. If you worry at all about due process, facing your accuser, etc., don't bother to move here.