explicit targets based on measurements and must interface with the evaluation team.

- Ensure your evaluators are not particularly enthusiastic or cynical about the new technology being evaluated. They need to be motivated by the requirements to ensure the successful completion of the evaluation exercise not the adoption or not of the technology. Often companies have *technology champions* who assess and promote new technology. A champion in this sense should not be in charge of an evaluation exercise he/she will have too much vested interest in specific "pet" technologies. An evaluation needs a *process champion* who is not concerned with particular technology but with ensuring the best overall development process for the organisation. A process champion should be as concerned to avoid bad process changes (i.e., non-beneficial or unnecessary changes) as to adopt good process changes.

CONCLUSIONS

This article has identified a number of human factors and sociological issues that can distort the results of an evaluation exercise. When you undertake an evaluation exercise, you need to be sure that you have identified all such effects and put in place specific processes to minimise their impact.

The next few articles will describe some of the detailed techniques for performing feature analysis and quantitative case studies.

REFERENCES

[1] H.M. Parsons. What happened at Hawthorne? Science 183, pp922-932, March 1994.

Editor's Filler

After reading this article, you have to ask yourself one question ...

Are software engineers human?

Risks to the Public in Computers and Related Systems

Peter G. Neumann, Moderator

Edited by Peter G. Neumann (Risks Forum Moderator and Chairman of the ACM Committee on Computers and Public Policy), plus personal contributions by others, as indicated. Opinions expressed are individual rather than organizational, and all of the usual disclaimers apply. To economize on space despite the enormously increasing volume of cases, we tersify many items and include on-line pointers to other items in the on-line Risks Forum, where (S i j:p) denotes *SEN* vol i no j page p, and (R i j) denotes RISKS vol i number j. The RISKS archives are available on ftp.sri.com, cd risks. Please send RISKS-related items to risks@CSL.sri.com. Read RISKS as a newsgroup (comp.risks), or subscribe via the automated listserv at risks-request@CSL.sri.com. Peter G. Neumann, SRI International EL-243, 333 Ravenswood Ave., Menlo Park, CA 94025-3493 (1-415-859-2375; neumann@csl.sri.com).

Largest computer error in US banking history: US$763.9 billion (David Kennedy)

When Jeff Ferrera and Cindy Broadwater checked their checking balance at the First National Bank of Chicago, the automated voice gave it as $924,844,208.32. More than 800 other folks had similar stories to tell. The sum total for all accounts was $763.9 billion, more than six times the total assets of First Chicago NBD Corp. The problem was attributed to a "computer glitch". [Source: AP US & World, 18 May 1996, By Mario Fox, Courtesy of Associated Press News via CompuServe's Executive News Service. PGN Abstracting. The title of this item is inspired by the American Bankers Association, noted by Dave Tarabar. PGN]

(Louis Koziarz:) The 'glitch' was apparently the result of a programming change intended to support the new out-of-area ATM fees being proposed by various banking groups. When the new transaction messages were introduced to the network, some systems took the strange new codes and transformed them into something they could understand: a posting of a huge credit to one's account.

Computer Error Costs MCI $Millions (Scott Lucero)

In *The Washington Post*, 29 March 1996, MCI reported that they will refund approximately $40 million due to a computer error. A billing error was uncovered by an investigative reporter from local television station, WRIC in Richmond, VA. The reporters found that they were charged for 4 minutes after making a 2.5 minute call, leading to an in-depth investigation.

Western U.S. power blackout (PGN)

More than a dozen states including California, Oregon, Washington, Utah, Nevada, Wyoming, Arizona, reported power outages on 2 July 1996. At least 11 separate power plants "inexplicably were knocked off line". The problem appears to

have originated at a 1500-megawatt intertie at the California-Oregon border. Later in the day, plants in Rock Springs, Wyoming, and along the Colorado river also went off line. [Source: Reuters item, *The Boston Globe,* 3 July 1996, p.3]

On the following day, parts of Idaho were again blacked out. Perry Gruber, spokesman for the Bonneville Power Administration in Portland, Oregon, said, "We can rule out sabotage. We can rule out UFOs. I think we can rule out computer hackers." Utility officials said it may take as long as a week to find the cause(s). [Source: Associated Press item, *The Boston Globe,* 4 July 1996., p.4]

(Jerry Saltzer, in Idaho at the time:)

What was most striking was the sheer confusion in reports of what might have been the cause. AP reported without comment that eleven generating plants shut down simultaneously, with the apparent implication that some kind of widespread conspiracy was involved. Idaho Power said the problem originated in California, but its system autoshut down completely and had to go through a 'Black Start'. Oregon's main power company said it was a problem on the Pacific Northwest Intertie. Colorado's power company said the problem originated in their system but they didn't understand what it was. Idaho Power said it had nothing to do with the hot weather and unusual load from air conditioning. Oregon said it was caused by the hot weather and unusual load from air conditioning. Three days later they still didn't have any consensus on what had happened. Impressive disarray–one has the feeling that they don't talk to one another. With this much lack of communication, I'm not sure they should be allowed to interconnect, either.

(PGN, postscript:) It took until 20 July 1996 – 18 days later – for the cause to be identified officially: *an Idaho transmission line that short-circuited when electricity jumped to a tree that had grown too close.* The tree, which has since been removed, caused a flashover in an area about 100 miles east of the Kinport substation in southeastern Idaho. The line carried 345 kilovolts. [Source: Associated Press item in the *San Francisco Sunday Examiner and Chronicle*, 21 July 1996, A-8.]

(Nicholas C. Weaver:)

At least 1.5 million customers were affected by sporadic outages. Apparently an instability in the power grid caused these problems. (It is interesting how sporadic these outages were. In Berkeley, our power wasn't interrupted, yet portions of the Bay Area subway system (BART) were without power).

The great Netcom crash (David Lesher)

Netcom, Inc; one of the largest retail ISP's [450,000 subscribers, 230 POPs] went down for 14+ hours during the week of 17 Jun 1996. In what strikes me as "shades of Mariner II" Netcom President David Garrison, appearing on KGO Radio said it was an extra "&" in the "border gateway protocol code" in the MAE-East router in DC area that killed the system. They had to bring down all 100+ routers & flush each one to recover, he reported.

The parallel with the Bell Atlantic STP bug of about five years back strikes me. The routing nut has gotten so tough that the tools used on it can be very rapidly fatal.

Microsoft, AOL, and AT&T also have netwoes (PGN)

An article by Peter H. Lewis in *The New York Times,* 24 Jun 1996, p. D1, noted the Netcom problem ("for 12 hours"). The article also noted these other problems:

- Microsoft shut down its nationwide network on Sunday (presumably 23 Jun 1996) for 10 hours as part of an intended backup power-supply upgrade, but the upgrade failed and they will have to try again.
- America Online was out of service for an hour on 19 June "1996, when a planned system software upgrade backfired."
- AT&T will shut down its Internet access for up to 8 hours each week, for maintenance.

MARTA train jumps track (Stephen Cohoon)

On Saturday, 1 June 1996, a commuter train operated by the Metro Atlanta Regional Transit Authority (MARTA) had one car leave the track causing injuries to 19 people and much embarrassment for the "Official Spectator Transportation System" for the Olympic games. According to local TV news and newspaper reports, the train had stopped before a red signal apparently on automatic control. The operator called dispatch requesting permission to go to manual. Permission was granted and the operator proceeded *through the red signal* setting off alarms. The train was stopped and put into reverse. As one of the middle cars passed over a crossover switch some or all of its wheels were lifted and displaced. The train stopped very suddenly tossing the operator and 18 passengers from their seats. MARTA does not consider this a derailment because no cars fell on their sides.

A MARTA person interviewed on camera said there is no time that any train on manual or automatic should pass a red signal. The operator, the supervisor on duty and the dispatcher have been suspended pending a review.

Personal opinion: this is a familiar scenario often repeated in RISKS but apparently not yet learned by those responsible for critical safety systems. Operator training and supervision must exceed the the capacity of a system to cause harm to people. Manual overrides must be designed to increase safety not allow safety systems to be subverted.

Taipei subway computer crash (Calton)

Taipei's only subway line service was completely disrupted on Monday morning, 3 June 1996, due to the simultaneous shutdown of both the main computer and the backup system. The control center ordered an emergency shutdown of the entire system, which did not cause any train accidents or casualties. The subway company reported that at 9:27am on that morning, the main control computer suddenly printed out 14 pages of extraneous program code. Eight minutes later, both the main control computer and the backup system went down. Maintenance engineers, with the help of a Matra engineer (the company that supplied the control software), were unable to reboot either system. Digital engineers (the company that

supplied the hardware) arrived shortly and discovered that one of the rebooting programs was missing. They reloaded the rebooting program from backup media and the subway line/system returned to normal functions after four hours and thirty-four minutes.

The situation is complicated by the recent breakdown in contract negotiations between the subway company and Matra for maintenance. Matra has taken back most of its maintenance personnel, but the subway company has not fully acquired the capability for maintaining the entire system, including the computing system, particularly the proprietary control software written by Matra.

The subway company presumes the incident to be sabotage and has asked the police authorities to investigate. The police computer experts have declared that it is difficult to investigate the control software consisting of more than ten millions lines of code. Furthermore, the police have not ruled out the other possibilities such as operator error and software design error.

In the public opinion section of the same newspaper, several readers discussed the risks involved in this kind of incident. The section title was "The important question is: who should be responsible for computer security", subtitle "who sabotaged the computer is secondary." (Source: digest/translation of news from United Daily News, Taipei, 5 June 1996.)

Ariane 5 failure (John Rushby)

Faulty computer blamed in Ariane 5 rocket failure: Experts studying the moments before the Ariane-5 rocket explosion say faulty computer software may be to blame for the rocket veering off course. Apparently, the rocket was misfed information that made it think it was not following the right path. The rocket then changed direction, causing the upper part to began to break apart. (From CNN's web page www.cnn.com)

(Andy Fuller:) According to the 24-30 June issue of *Space News,* the 4 June 1996 explosion of the Ariane 5 rocket was caused by software in the inertial guidance system. Apparently an inertial platform from the Ariane 4 was used aboard the Ariane 5 without proper testing. When subjected to the higher accelerations produced by the Ariane 5 booster, the software (calibrated for an Ariane 4) ordered an "abrupt turn 30 seconds after liftoff", causing the airframe to fail.

The article notes that a request to test the inertial platform under conditions similar to those produced by the Ariane 5 was "vetoed by CNES for budgetary reasons." Sextant Avionique, the builder of the inertial platform, has since performed these tests and confirmed that it would fail in an Ariane 5 launch. We are again reminded that crashing a simulator is lots cheaper than crashing a vehicle. [See other discussion in (R 18 18 and 22).]

Matra made software for Ariane5 and Taipei subway system (Frank Rieger)

The German newspaper *Tageszeitung* reports in its issue of 6 June 1996 (6/6/6!) that the software for the engine-controlling in Ariane 5 was made by the French company Matra Corp. This is the same company that made the software for the Taipei subway system that crashed on 3 June 1996.

First statements from DASA, ESA and ArianeSpace say that after 37 seconds there was a movement of all engines in one direction, causing the Ariane 5 into an extreme flight position. This disrupted the main structure of the vehicle and triggered an automated destruction mechanism. Some seconds later the manual destruction from ground control was triggered by the flight security officer for redundancy. According to German press agency Deutsche Presse Agentur, one manager of the French space agency CNES stated that the computer has tried to compensate a nonexistent problem in flight control by making this massive move.

So, for me there are two possible reasons for the crash: there was an sensor failure, transmitting false data about the external conditions (wind, flight position) to the control system, or there was an real software 'glitch' causing the critical failure. On the basis of the information available now, I ask myself, why was there no mechanism to avoid the control computers' attempt to go into this extreme flight position?

[Note added later: The leading European TV-Satellite corporation ASTRA has chosen Matra Corp. as hardware/software supplier for their next generation of digital broadcast satellites... (Source: Deutsche Presse Agentur). FR]

Martinair B767 Aircraft suffers EFIS failure (Peter Ladkin)

Flight International (5-11 June 1996, p8) reports that the crew of a Martinair B767-300 registration PH-MCH 'faced blank flight-instrument displays' near the US coastline on a flight from Amsterdam to Orlando, FL on 28 May 1996. Apparently it had suffered an EFIS failure (EFIS is the industry acronym for the system which displays the flight data on screens in front of the pilots – a feature of most modern transport aircraft. The EFIS failure itself was not such a big issue. The plane continued on the electro-mechanical standby instruments and diverted to Boston, where it landed safely – but very fast, with no flaps, spoilers, autobrake or anti-skid. It burst 8 mainwheel tires and the brakes caught fire (neither event unusual in a fast landing and heavy stop) and the fire was quickly extinguished. Martinair said the crew employed 'flaps one', which extends leading-edge spoilers only, and that they had no reverse thrust.

Martinair said the aircraft had a partial DC-power failure, but an unnamed 767 captain apparently said that such an event would not cause an EFIS failure. Boeing said reports of a complete power failure are 'not confirmed'.

NY Air Route Traffic Control Center computer failure (Peter Ladkin)

The NY ARTCC computer (7 years old) lost significant service capability ('failed' said *The New York Times Service*'s Matthew Wald on 21 May 1996) twice on the evening of Monday 20 May; the first time for 23 minutes, and the second time for about an hour, one hour later. The *NYTS* reported

(*International Herald Tribune,* 23 May 1996, p2) that it was 'running normally' Tuesday as technicians tried to figure out the problem. The FAA is wondering about the new software installed four days earlier. 'The office, the New York Air Route Traffic Control Center, handles high-altitude and long-distance traffic over New York, Connecticut, New Jersey, Pennsylvania and part of the Atlantic Ocean.' (Wald, NYTS, 21 May 1996)

There followed the usual: a fail-safe return to older, more inefficient air traffic control procedures, leading to a lower traffic saturation limit and thus mean delays in departures of about an hour at major airports in the area; an increase in the work load of controllers; a deficit of safety-related information, including 'automatic conflict alert'.

I note that a deficit of safety-related info does not necessarily lead to a reduction in safety: one increases safety margins and pays careful attention (which might even increase safety for the short periods involved). These older procedures worked tried and true for decades. Risks might increase were an ARTCC system to suffer a service reduction at a time at which there were more aircraft in the system than the saturation limit for the reduced level of service. Aircraft in the air already under control do not just go away, however one can delay entry into Center control by delaying aircraft ready for departure and diverting flying traffic due to enter Center control (but note the huge area NY ARTCC covers). I am not aware that such a circumstance has ever occurred, but given the projected growth in commercial air traffic, it is something to worry about for the future.

[Computers and ATC were discussed in RISKS-17.17 (James), 17.18 (Wolper), 17.21 (Burstein, Schultz), 17.24 (PGN), 17.25 (Runes, Karagianis, Ladkin, Pettit), 17.26 (PGN, Margolin, Zellweger), 17.27 (Gelato), 17.28 (PGN), 17.35 (Lucero), 17.36 (Tignanelli, 2 articles), 17.38 (Ladkin), 17.40 (PGN, Ladkin), 17.41 (Tignanelli, Emerson), 17.44 (Goldstein, see also Harding, Menon), 17.49 (PGN), 17.50 (PGN), 17.62 (Kabay), 17.70 (Wolper). ATC Communications were discussed in 17.44 (Harding, Menon), 17.64 (Lucero), 17.65 (Ladkin). PL]

FAA drops navigation system contract (Fred Ballard)

Citing cost overruns and schedule delays because of mismanagement, the Federal Aviation Administration canceled a $475 million contract that was intended to help the airlines get extremely precise navigational data from satellites. The FAA announced the contract in August with Wilcox Electric Inc. of Kansas City, a subsidiary of Thomson-CSF SA of Paris. The FAA said the action was part of a new strategy of cutting losses early, rather than struggling along for years with mounting delays and cost overruns. [Source: *The Minneapolis Star Tribune*, Saturday, April 27, 1996, p. A8.]

Massive failure of Washington DC traffic lights (Jeremy J Epstein)

According to *The Washington Post,* 9 May 1996, most traffic lights in downtown Washington D.C. went onto their weekend pattern (typical: 15 seconds of green per light), rather than their rush hour pattern (typical: 50 seconds of green per light). This occurred during the Wednesday (8 May) morning rush hour. The problem was reportedly caused by a new version of software installed in the central system that controls all of the traffic lights, providing timing (so lights turn green in sequence). The result was mile-long traffic jams. One woman reported that her 35-minute commute turned into 75 minutes, due to the overloaded streets. By the afternoon rush hour, the software glitch had been "fixed". It wasn't clear whether that meant they reloaded the old software or fixed the bug.

Some might consider this a risk of computer controlled systems, and others might consider it a substantial increase in the nation's productivity: think of all the lawyers and congresscritters who couldn't get to work!

Workmen strike at CERN (Al Smith)

After a shutdown of 6 months during which the LEP vacuum system was opened at many locations, the accelerator was started up on 14 June 1996. After 5 days of machine studies, it became clear that there was an obstacle inside the LEP vacuum chamber close to Point 1. On the morning of 19 June the vacuum system was opened and 2 empty beer bottles, some 5 metres apart, were found inside the beam pipe. This incident has caused a 5-day delay in the setting up of the accelerator and will result in a reduction of about 10% of the time available for running LEP2 at the W pair production threshold (161 GeV) in 1996. [Low-tech glitch in a high-tech environment. They need a lager logger? PGN]

Xerox machine caused nuclear-power plant emergency halt (Magnus Ihse)

One of the Swedish nuclear reactors, Ringhals 4, was automatically shut down during a routine safety check. The last part of the instructions fed into the computer was missing, and when the computer safety system noticed that the instructions were incomplete, it shut down the reactor.

So far so good, but why were the instructions incomplete? The Xerox machine used to copy the instruction sheet did not include the complete page, and no one (except the computer) ever noticed that the instructions were incorrect. (Source: TT)

The risk is obviously that no system is completely fool-proof. I doubt anyone ever thought about the correctness of the Xerox machines as part of the nuclear power plant safety system. No matter how detailed you planned the security system, there will always be some part that could fail. In this case, nothing serious happened because the computer detected the error. However, this – or similar incidents – could happen again, and next time maybe the error would not be detected.

US Charges Man Planned to Kill 4,000 Travelers (Reuter) (PGN)

Reuter reported on 29 May 1996 that U.S. prosecutors accuse Islamic militant Ramzi Ahmed Yousef (a.k.a. Abdul-Basit Balochi) and two others of plotting to bomb 12 U.S.

jet planes in two days during 1995. Some of the evidence is based on a file found in Yousef's laptop computer, stating that the purpose of the bombings was "vengeance and retribution" against the United States for its financial, political and military support of Israel. (Yousef will be tried later this year for masterminding the 1993 World Trade Center bombing that killed six and injured more than 1,000 people. He is also accused of placing a bomb on a Philippine Airlines flight from Manila to Tokyo on 11 Dec 1994, which killed one passenger and injured 10 others.)

Data entry omission extends prisoner's sentence (James K. Huggins)

John O'Valle was convicted in 1987 on charges of cocaine and weapons possession, and was expected to serve 20 years in prison. Later on, however, the sentencing judge reduced the sentence on technical grounds, making him eligible for release in 1992. The reduction was noted in O'Valle's written file, but not in the Department of Corrections' computer records. (Neither O'Valle nor his lawyer was notified of the change.)

In January 1996, prison officials reviewed his records and discovered the discrepancy. However, there is now a new problem. In 1995, O'Valle was convicted for possession of marijuana while in prison, a felony. Had he not been in prison at the time, he would have been guilty of a misdemeanor and not subject to jail time. So now O'Valle is serving time for a felony, which (presumably) never would have happened had he been released on time. State officials aren't sure what to do.

Officials aren't sure what happened. O'Valle's warden says that sentencing formulas are complicated, and the prison camp program and parole programs were in "transition" during the time O'Valle entered the system. [Summarized from the *Detroit Free Press*, 11 April 1996, p. 4B.] this is a new story with an old moral: if you have replicated data sets, make sure that the data sets are consistent.

Baltimore throws the book at criminals (Peter Wayner)

Baltimore just finished creating a brand new technologically advanced "central booking" building where police take people after they've been arrested. Unfortunately, this heavily computerized system has become media fodder lately as people get lost in the building and are not released for days. I've seen one television news report that interviewed a woman who said she spent five days in the building because of a minor warrant for an unpaid fine. Bail was posted several times and lost.

The Thursday 18 Apr 1996 edition of the *Baltimore Sun* reports that the system is now working faster after the police started overriding the computers. For instance, there was an automated system by which prisoners could be called up for their hearings. The handheld computers that carried these messages, however, didn't work and now the City has detailed five extra officers to escort the prisoners instead.

Another woman complained that her 18-year-old retarded child was held a full day after bail was set. She says that she was speaking with booking center over the telephone when the child knocked at the door. The booking center was telling her that her son could *not* be released until all of the computer records were complete. I can only hope that the same glitch won't let out a dangerous criminal.

The article ends by noting that the District Court Commissioner says that "Anybody [who's] been in this building would be a damn fool to [go] back to it."

Swedish court fines parents for son's overly long name (Li Gong)

It is well known that numerous computer programs are so poorly designed and implemented that they cannot handle special cases of people's names (e.g., the case of the person simply named "Smith" (R 18.05)). In some other cases, there are real physical (and other) constraints that are hard to code around, such as in the case of some colleagues whose long names risk falling off the edge of their company badges. Sometimes people just push things to far to the extreme. The *Guardian Weekly* reported (in the issue ending 21 Apr 1996, p.4) that "a Swedish court has fined a couple $660 for breaking the law by naming their son Brfxxxcccxxmnnpccccllllmmnprxxvvclmnckssqlbb11116– or Albin for short." [See items from Viiveke F?k ('?' is =E5) and Gunnar Pettersson discussing the Swedish Name Law (R 18 07). PGN]

Australian court emulates Swedes (Ashley Robertson)

A similar situation has occurred here in Western Australia. New parents of a baby boy were unable to give their child an ancestral name because of the accents on some of the characters. The name was not offensive or difficult to pronounce. The reason given was that the computer system of the Registry of Births and Deaths could not accept the name because it was not a standard ASCII character.

The solution was not as easy as removing the accents because that substantially changes the pronunciation of the name. The child remains unnamed!

AOL censors British town's name! (from Clive Feather)

Clive forwarded to RISKS an long item from the Computer underground Digest, Thu Apr 11, 1996, Volume 8 : Issue 29, ISSN 1004-042X, from Doug Blackie that relates an experience Doug had in trying to register with America On Line. He entered his name "Blackie" and his home town "Scunthorpe", and found that AOL's (indecency-filtering) registration program would not accept that combination. After various discussions with the AOL folks in Dublin, he discovered that he could register properly if he entered the town as "Sconthorpe". As a result of this curious situation, AOL has announced that the name of the town will henceforth be known as "Sconthorpe". The entire saga is documented in the Scunthorpe Evening Telegraph (final edition) of Tuesday, 9 Apr 1996, issue number 30111, printed and published by Grimsby and Scunthorpe Newspapers Ltd., Telegraph House, Doncaster Road, Scunthorpe, DN15 7RE, UK. The article was provided on-line by David G. Bell, and was included as a part of Doug Blackie's message. PGN Abstracting. See fol-

lowup discussion in the on-line Risks Forum (R 18 07,08,10) – including the offensive 'Am' in 'America' in Turkish and 'Sconthorpe' in French. There are no easy answers to this problem, especially internationally. PGN

The "finger" command and "Paul Hilfinger" (Jim Horning)

The AOL censorship item reminds me of Paul Hilfinger's story about the time the Carnegie-Mellon University computer-center staff was ordered by the CMU administration to change the name of the "finger" command (despite it being an ARPAnet standard). They changed "finger" to "where" and also took it upon themselves to change Paul's name to "Paul Hilwhere" (initially intending it to be temporary). Paul actually approved of the change (as a kind of gentle protest), and it remained that way for some time.

Filename bug in Windows 95 (Vsevolod Ilyushchenko)

I have found a serious bug (feature?) in Windows 95. It does not properly treat files that contain certain characters in their names. These characters include those with ASCII values of 255, 254, 249, 244, 23* and some others, all above 127. I have not found a common rule (so I probably failed the Microsoft IQ test).

This problem was noted by Olcay Cirit (S 21 4:17 and R 17 64) in regards to ASCII 229. He wrote that if this character is the first in a filename, then the file cannot be deleted, copied, renamed or executed. Actually, *any* of these characters at *any* place in the filename will spoil the file. Such files are visible in Explorer, with bad characters shown as underscores. You can create shortcuts to them, view their properties or even try to rename them. But any serious operation has to be performed from the command line.

A peculiarity of my DOS file managing program is that it uses direct disk access to delete files. I could not do that under Windows 95 until recently, so to deal with the "bad characters" I had to reboot into DOS prompt. Then I discovered the the "LOCK" command will allow DOS utilities to access disk directly. However, this is probably an undocumented command, it's absent in the DOS help file, and it is not an executable file.

A note for those unfamiliar with the "funny" characters. You can enter any character at the DOS prompt by holding the Alt key and pressing the keys with digits for the character at the numeric keypad. For example, Alt+097 is 'a', and Alt+255 is one of the "bad characters". So, to see the described behaviour for yourself, create at the DOS prompt a new file that has a "bad character" in its name, then try to do something with it in Windows 95.

The risks? Aside from user confusion and possible pranks (which cannot do much harm, because you can always go to the command line and fix the things), there is another issue. Usually filenames with "bad characters" are not used. However, here in Russia one way of russifying a PC is to replace all those Greek, German and Swedish symbols that reside in the upper part of the ASCII table with Russian letters. So, if a Russian user had many files with Russian names, and then switched to Windows 95... Surprise, surprise! You can't manage your old files there.

Telephone accounting (Warrick Jackes)

A Brisbane bloke was stunned to discover on his latest phone bill an amount of nearly $900 for a call of more than 10 hours duration to the Solomon Islands. The bloke *does* occasionally call the Solomons and *does* admit to being a bit of a yakker [talk the doors off a barn]. But for 10 hours? Query with Telstra [read as Bell Australia] brought the testy advice that he must have forgotten to hang up his receiver. The bloke pointed out that this theory was flawed by Telstra's own bill that showed that he'd used the same phone to call Melbourne (Australia) only 11 minutes after the start of the call to the Solomons. [*Sunday Mail* (Brisbane)", Sunday, the 14th April 1996, page 12]

This case apparently stirred Telstra into prompt action. By Monday, 15 April, the matter had been "investigated" and the charge waived. [*Sunday Mail* (Brisbane)", Sunday, the 21st April 1996, page 12]

When the Clock Strikes 2000 (Edupage, 23 Apr 1996)

The Gartner Group in Stamford, Connecticut, says the federal government will spend about $30 billion to modify a massive number of computer programs in which years were coded simply as two-digit numbers (without identifying the century) and which will have to be fixed so that they can correctly calculate things like benefits payments. It is also estimated that by the time the year 2000 comes around only 70% of government computer programs will have been modified to deal with the problem. (*Computerworld,* 22 Apr 1996 p1) [We previously noted estimates of something around half a trillion dollars worldwide, also from the Gartner Group (S 21 2:16: and R 17 82). PGN]

ONE-LINERS:

- GPS will roll over to 6 Jan 1980 at the end of 21 August 1999 (R 19 24)
- More daylight savings time problems (R 18 02-05)
- Discussion of Cali and Puerto Plata B757 crashes (R 18 10)
- Accidental shootdown of one Japanese F-15 by another (R 17 65, R 18 18)
- Intel shut down by power-company software bug, 5-hour outage (R 18 02)
- Health risks from dusty computer displays (R 18 21,23)
- General Motors recalls almost 300K cars for engine software flaw (R 18 25)
- Computer error in Cape Town election affects results (R 18 17)
- Report on risks in electronic voting in Iowa by Doug Jones (R 18 15)
- "tif" to "jpg" fix results in arjpgicial, idenjpgied in Sydney paper (R 18 24)
- Joe Klein's computer-detected authorship of Primary Colors (S 21 4:14) confirmed by handwriting analysis of typescript annotations, then finally acknowledged by publisher! (R 18

26)
• MS Word grammar checker suggests *rigor mortis* for *school reviews* (R 18 24)
• MS Mexico recalls offensive Spanish-language thesaurus (R 18 25)
• Computer aspects of Credit Lyonnais Fire discussed (R 18 14)

SECURITY AND PRIVACY

NYPD phone system cracked (Fernando Pereira)

The AP reported that, according to the *New York Post*, 19 Apr 1996, callers to New York Police Department headquarters for 12 hours ending 6am Tuesday [16 Apr 1996] heard a bogus recording that included the following: "You have reached the New York City Police Department. For any real emergencies, dial 119. Anyone else – we're a little busy right now eating some donuts and having coffee." It continued "You can just hold the line. We'll get back to you. We're a little slow, if you know what I mean. Thank you." The NYPD had no immediate comment, but unnamed police sources believe hackers broke access controls and changed the message.

TILT! Counterfeit pachinko cards send $588M down the chute (Peter Wayner)

The *Wall Street Journal* of 22 May 1996 (A18) reports that two Japanese firms lost about 55 billion yen when criminals counterfeited the stored money cards that they manufactured. These cards are used to pay for pachinko games, but you can get refunds wired to an account if you cash in a card. If my memory serves me correctly, there is a certain amount of skill involved. If you play well or are lucky, you might even add money to the cards. But I'm not sure about this detail. In any case, the people with the counterfeit cards could get refunds when they didn't pay for the original card.

The Journal mentions three interesting details. First, the cards were pushed by the police as a means to track the flow of cash and stop money laundering. Obviously, there wouldn't be these losses if they could really track the flow. Second, the convenience of the new cards initially boosted profits because it was so much easier to play with the cards that automatically kept track of your money. Finally, the Journal reported that there are 18,244 pachinko parlors in Japan.

[Chiaki Ishikawa added some fascinating details in the on-line RISKS (R 18 16). See also an article by Andrew Pollack, Counterfeiters of a New Stripe Give Japan One More Worry; Fake Cards Thwart Efforts to End Pinball Scams *The New York Times*, 20 Jun 1996, D1.]

OS/2 Warp TCP/IP misfeature (Pete Bentley)

It seems that in the OS/2 (2.1 and Warp) TCP/IP stack socket descriptors are system-wide. That is, they aren't per-process file descriptors, so if you can discover the number of some other process's socket (and netstat -s will helpfully list all the open sockets on the system) you can send(), recv(), shutdown() or do many other fun things with it.

The risks include the fact that anyone with telnet access to the machine (and OS/2 telnet security is a risk in itself) can write a program to subvert any TCP/IP server running on it. It is a shame, because otherwise it's one of the better non-Unix implementations of the BSD socket API.

Government computer break-in in Australia (David Kennedy)

Thieves Raid Government Building: Computer thieves raided one the Queensland government's most sensitive buildings on 18 May 1996, in Brisbane, ransacking three floors and dismantling around 55 computers, police said. A spokesman for Premier Rob Borbidge said the break-in at the executive building annex in George Street had prompted a review of security at all government buildings. The spokesman said the break-in in the sensitive treasury area did not appear to be politically motivated. [Australian Associated Press, 18 May 1996]

Massive cell-phone identifier interception (PGN)

Two people in Brooklyn NY (Abraham Romy and Irina Bashkavich) were charged with stealing over 80,000 cellular phone numbers, along with corresponding identifying serial numbers and personal identification numbers, using a scanner (digital data interceptor) from their 14th-floor windowsill above the Belt Parkway in Brooklyn. Police seized two handguns, six computers, 43 cellular phones, and the scanner. Cellular-phone fraud reportedly amounts to losses of $1.5 million per day. [Source: An Associated Press item in *The New York Times*, 3 July 1996, p. B4]

Judge: Computer encryption codes ruled protected speech (Jay J. Kahn)

U.S. District Judge Marilyn Hall Patel released a ruling on 16 Apr 1996 that mathematician Daniel Bernstein could try to prove that the U.S. export controls on encryption technology are too broad and violate his right to communicate with other scientists and computer buffs – a right protected by freedom of speech. (Bernstein's cryptographic programs are called Snuffle and Unsnuffle. The U.S. State Department decided in 1993 that Bernstein's written article and programs required export licenses [because crypto purveyors are considered as being international arms dealers under ITAR], but later backed down on restricting the article; Bernstein then had sued for release of the programs.)

David Banisar of the Electronic Privacy Information Center (EPIC) is quoted in the news item: "It's important to recognize that computerized information has the same kind of legal protection that printed information has." [Source: http://www.usatoday.com/news/nds19.htm; PGN Abstracting]

56-Bit Encryption Is Vulnerable, Says Phil Zimmermann (Edupage)

Philip Zimmermann, creator of Pretty Good Privacy encryption software, testified before a Senate subcommittee that, based on a 1993 presentation by Michael Wiener of Northern

Telecom, it would be possible to build a machine for $1 million that could crack a message encrypted with the Data Encryption Standard and a 56-bit key in an average of 3.5 hours. A more powerful machine, costing about $10 million, could do it in 21 minutes, and a $100 million machine could bring the time down to two minutes. Zimmermann's testimony contradicted a recent statement by U.S. Attorney General Janet Reno that even with a "top of the line supercomputer, decoding a 56-bit key would take over a year and the evidence would be long gone." At issue is whether the U.S. should permit the general-license export of 56-bit encryption products. (BNA Daily Report for Executives 27 Jun 1996, A5, in Edupage, 30 June 1996)

Federal Court rules against Communications Decency Act (Marc Rotenberg)

In a ruling likely to have a significant impact on the future of the Internet, a special three-judge federal court declared on 12 Jun 1996 that the Communications Decency Act is unconstitutional on its face. The landmark decision came in a legal challenge initiated by the ACLU, EPIC and 18 other plaintiffs. EPIC is both a plaintiff and co-counsel in the litigation. The ACLU/EPIC case was consolidated with a subsequent action filed by the American Library Association and a broad coalition of co-plaintiffs.

Their lengthy ruling consists of separate opinions authored by the three members of the federal court panel. While the three judges differed in their approaches to the legal issues raised in the case, they were unanimous in their strong conclusions that the CDA constitutes a clear violation of the First Amendment. A complete copy of the opinion, as well as selected excerpts and related news items, can be found at http://www.epic.org/ .

ONE-LINERS:

- Risks of being indexed by search engines (R 18 15)
- Risks in altered live video images: L-vis Lives in Virtual TV (R 18 18-21)
- National Research Council crypto study report available from National Academy Press; see http://www2.nas.edu/cstbweb for summary (R 18 14,17)
- Case of Oracle wrongful termination based on e-mail evidence (R 18 07-08)
- UK libel writ served overseas by e-mail (R 18 09)
- Discussion of New Orleans police chief murdering accuser despite wiretap (Shabbir Safdar, R 18 01)
- Intruder hacks into Cambridge University systems (R 18 09-10)
- St. Louis teenager Christopher Schanot arrested for computer fraud (R 18 01)
- Two convicted: 1,700 Tower Record credit-card numbers offloaded (R 18 02)
- John Munden, UK policeman, acquitted after having his bank account cleaned out and false fraud accusation. Must read this one. (R 18 25)
- Australian insurance company builds household database from electoral rolls (R 18 02)
- Software piracy considered enormous, Hong Kong, worldwide (R 18 12-13)
- Cyber-terrorists blackmail banks and financial institutions (article with considerable hype) (R 18 17,24)
- *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, GAO/AIMD-96-84, in Senate hearings (R 18 15)
- Filegate privacy issues involving FBI, Secret Service, White House (R 18 21)
- South Korea clamps down on Canadian home page on North Korea (R 18 21)
- French police raid leading Internet service providers (R 18 21)
- Laptop with unspecified data stolen from London police car (R 18 24)

Following the Java and Netscape problems reported in the previous issue (Dean/Felten/Wallach, Hopwood) and JavaScript (LoVerso), there were further problems reported in Java and JavaScript (R 18 09), in Netscape 2.02 (R 18 13,14), and again in Java (Hopwood, R 18 18). There is also further discussion of security and privacy implications of "cookies" (squirreled information in browsers) (R 18 19,20).

Editor's Filler

Ah yes!

Another breadth of insanity!

Thank you Peter ... It seems we continue to be part of the problem, not the solution.

Now onto the workshop summaries ... good stuff.