2600

JUNE, 1986

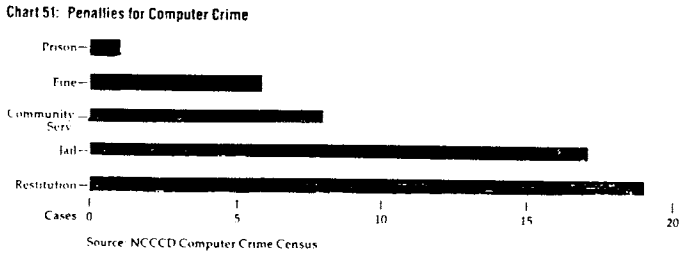
VOLUME THREE, NUMBER SIX $2

Computer Crime Review

The National Center for Computer Crime Data, purveyors of computer crime wisdom, have assembled a statistical report entitled *Computer Crime, Computer Security, and Computer Ethics.*

This report, the first such one, reviews measurable trends in computer crime and computer use. It does this using graphic representations to present its information accompanied by brief introductions.

The National Center for Computer Crime Data's (NCCCD) report is an excellent guide for those who are setting computer policy around the country—in industry, in government, and through user groups. It provides some empirical basis for the 'War Game-ish' attitude that is usually taken by the computer illiterate facets of computer power—namely industry and government. In a form that can easily be digested by the illiterates, the report includes seemingly irrelevant data (to computer users) that, in fact, provides background that the illiterates need. This is especially true for the graphs of world wide semiconductor consumption, computer sales, projected robot population growth, and an undocumented map of federal communication networks. These all add to the message that we all know: "Computers are important."



One of the NCCCD Report's noticeable conclusions is that the amount of computer crime has increased, that few are punished for it, that we are becoming more and more dependent upon computers, and that there is little awareness of security, relevant laws, and security procedures.

This information, taken two-dimensionally, says that we should make many strong computer-oriented laws to protect our national interest—a War Games response.

Taken another way, the report tells us that computers are becoming a more significant part of society and are being taken for granted as is television, and as such, we should act cautiously when passing computer laws.

If computers are becoming so intrinsic in American and international life, we must think twice before legislating them. Stealing is bad, but BBS's and commercial databases have entered the realm of our First Amendment rights to free speech, and this is the most precious thing we have.

Perhaps our attention in the subject of computer crime should be drawn more toward industry. What are they doing with the information that they store? Why is their data so easy to steal? Should they be more responsible to those who are dragged along with the burden that they carry? If they want your credit history, bank statements, arrest records, and other "transactional data" so badly, why don't they take care of it once they have it?

Computer laws affect both the user and industry, but are sponsored only by industry. By lobbying for legislation, industry gains its semblance of security from laws and law enforcement agencies who know nothing about telecommunications and computers. Industry must do its part to strengthen its integrity against attack from a computer criminal and not depend on laws to do the job. As world powers (who is it who said "knowledge is power"?), companies often do not accept their responsibilities.

An example that is usually cited is the case of GTE-Telemail on Telenet. When Telemail was breached back in 1983, hackers said, "It was so easy that I could not resist." At that time all new Telemail accounts had a default password of the letter "A". A full six months later (even as people were being indicted), the default password was the same. By allowing this situation to continue (they were even aware of the trouble four months before computers were seized in October, 1983), Telemail's real intentions and real commitment to computer security were displayed. It is possible that this really reflects a lack of communication between GTE administrators and GTE programmers. Telemail was concerned enough to involve the FBI, make headlines, but not concerned enough to rectify the situation.

On a system as big as Telemail, it is almost criminal to have a one-letter password.

If we think about computers as more than just tools, as in the case of BBS's, we realize that we have to proceed with caution when it comes to computer laws. Anarchy will not result if we do not move fast, because it has always been a crime to steal money and government secrets.

The results in the report were drawn from information from 130 prosecutors' offices in states with computer crime laws. A major conclusion of the report is that computer crime has been "democratized". "The 'democratization' of computer crime does not mean that we no longer have to fear computer geniuses, just that we cannot limit our focus to them. Like every other type of crime, computer crime will ultimately reflect the culture that surrounds our computers." Computer criminals are not just hackers, but are employees, consultants, and programmers.

The most useful part of the report is the summary of all the provisions of the 45 state computer crime laws in an easy to read table.

The NCCCD is a research institute which studies all facets of computer crime. It was created to help answer legal, security, accounting, moral, and technological questions that computer crime poses. It publishes the Computer Crime Law Reporter, a collection of current computer legislation, and other publications.

Computer Crime, Computer Security, Computer Ethics. Jay BloomBecker, Editor. Available from the National Center for Computer Crime Data for $28 at 2700 N. Cahuenga Boulevard, Suite 2113, Los Angeles, California 90068. Call (213) 850-0509 for information.

How To Hack A Pick

"The closest thing to Pick in size and feel is probably UNIX. Both are big, complex operating systems that are migrating down to the microcomputer world after having been developed and refined on minicomputers. Both systems are sophisticated and very powerful, and both tend to produce vehement partisans. One of the big differences, though, is that UNIX partisans tend to be programmers, especially systems programmers. Pick's partisans tend to be users and applications programmers. Of the two systems, UNIX is the more powerful for scientific and engineering applications. Pick, by its structure, is better adapted for business and managerial applications.

"But Pick is hardly perfect. Structured programming purists shudder over the fact that Pick's only high-level language is an extensively reworked version of BASIC. The present release is multiuser, but not multitasking, and rather lacking in communications capability. Some of the UNIX-type concepts, such as pipes and filters, which are becoming widely available on other operating systems, are not fully developed in Pick. Software hackers generally dislike Pick because it is difficult to get inside the system and play with it." (BYTE magazine, October 1984)

The issue of security on Pick is not often considered, because there is almost no security on Pick. It is therefore very easy to crack a Pick system. Once a user has gained access to a system, he can peruse *all* of the data. Most people have not heard of the Pick operating system, but there are now 60,000 sites, 30 terrabytes of data, and 400,000 users. What is Pick, and who cares?

The Pick operating system contains many more functions than most. It has an English-like nonprocedural query language, a compiled BASIC language, a JCL-like procedure language called PROC, and a command line interpreter called Terminal Control Language (TCL). Pick runs on microcomputers (IBM PC-XT) and mainframes (IBM 308x, 43x1, etc.). However most Pick implementations are on minicomputers with five to fifty terminals. These are the most vulnerable to cracking, because they often have auto-answer telephone modems.

Once a cracker has a logon prompt from a Pick system, he can continue trying to login until he finds a valid user number and password. The system will not hang up after repeated failures. Passwords are almost always upper case letters, and often short. There is *always* an account called SYSPROG on every Pick system. This is also the best account to crack, because it has operator access to the system.

Perusing Data

After cracking the SYSPROG password, you can drop out of the menu to TCL. If there is no explicit option on the menu, the command "TCL" usually works. Type SORT ONLY DICT SYSTEM from TCL, and a list of all accounts on the system is displayed. To get a directory of the files on any account, type "LISTF (account)". To look through the items in the files, you must first make a pointer to the file in SYSPROG. Type "SET-FILE (account) (file)". Then type "COPY QFILE *" and when the system says "TO:", hit a carriage return.

Crashing the System

All that has to be done to crash any Pick system is to type control break until a "!" prompt is displayed. Type "6.079". Then, "=" is displayed, then type ".FF". All inputs are terminated by carriage returns.

Disabling the System

All Pick systems can be destroyed and rendered useless by the command "CLEAR-FILE DICT SYSTEM".

The September and October 1984 issues of *Byte* magazine give a good overview of Pick. The operating system has a unique data model and file structure, which is a bit complicated to explain in this limited space. Some books have also been published on Pick. There are Pick user societies and publications which would provide phone numbers for gaining access. In addition, many Pick vendors have on-line client system phone number lists—cracking a vendor's machine is a gold mine.

Pick vendors include Ultimate Corp., McDonel Douglass Software Systems, General Automation, Pick Systems Inc., and Datamedia. Richard (Dick) Pick is alive and well in California. There are also software houses which specialize in Pick, and they have Pick clients too. Users include K-Mart International and Harvard University.

nothing new in *computer underground*

The Computer Underground. By M. Harry. Available through Loompanics Unlimited. $14.95

by John Drake

The Computer Underground appears to be an excuse to publish text files. The book runs a long 257 pages of computer printout.

It is divided up into what M. Harry has written and what he has downloaded off a BBS. This is about a one to twenty ratio. It's also unfortunate that nearly everybody who writes about hacking spends so much time dwelling on the obvious—"this is a modem...there are 8 bits...you connect it to a phone line..." Even *Out of the Inner Circle* by Bill Landreth falls into this trap. There is nothing in Harry's writings that any self-respecting hacker/phone phreak doesn't already know.

I was hoping for real research like extensively tracing the beginning of phone phreaking through Captain Crunch, Abbie Hoffman, and *TAP* to the present, with some interesting interviews with hackers and phreakers. The only thing he seems to have actually done was to poll people through a BBS. His analysis of the results are also pretty obvious to anybody involved. He then proceeds to plot out the old flow chart of a searching and hacking program.

The rest of the 257 pages are printouts of text files. Harry seems to have a preoccupation with ARPANet and lists of dial ports. There is an abundance of blank space, particularly when a section ends at the top of a page. A few of the text files are typeset and nicely placed in the center of the page. The rest of *The Computer Underground* is mere printout, not even in double-emphasize mode. This is clearly not one of Loompanics' better releases.

New York's Computer Law

The New York Times

New York State legislators have reached agreement on a new computer crime law. The bill would create the new crimes of unauthorized use of computers, computer trespassing, and computer tampering. It would also make it a crime to use information stored by computer while committing other crimes, such as forgery or theft of business records.

Although 40 other states have already approved similar laws, legislation in New York is considered a major step in stemming computer crime in this country.

Since there are no such laws in New York, prosecutors must try to apply related law in cases involving computers.

A major provision of the bill, which is expected to pass the state Legislature and take effect next November, expands the legal definition of "written instruments" and "business records" to include computer data and programs. Under this change, penalties of up to four years in prison or $5,000 in fines would be imposed for these offenses: tampering with computer data while trying to commit a felony; making unauthorized duplications of computer material that deprive the owner of at least $2,500; tapping into legally confidential computer data.

The bill would also create several misdemeanor charges, punishable by up to one year in jail or fines of up to $1,000, to address low-level computer abuse.

Because many computer crimes occur across state lines, the bill includes a provision allowing New York State to prosecute an offender in another state who taps into a computer in New York.

$6,829 Phone Bill

The Hackensack Record

The 83-year-old retired insurance agent was quite surprised when he received a phone bill for $6,829.60. The 131 page bill was from GTE Sprint.

The man said that "the calls that I made are on the 129th page—for $29.49."

At last count the total on his account had risen to $67,594.02, a Sprint spokesman said, with 1,200 calls placed in one 24-hour period.

Sprint has a security department that monitors monthly bills and starts investigating when there is a fantastic change in use. The man's previous bills were about $20.

In this case, however, security did not cancel his code until three weeks after they noticed the increased usage.

Big Computer Crime Pays

Milwaukee Journal

One of the discoveries of a new study shows that when it comes to computer scams, the big-time crime pays. Two-thirds of the companies participating in the survey said that they tend to punish low-level employees accused of committing minor computer crimes while letting the major offenders go free.

"The cardinal rule seems to be: Thou shalt not steal small," says Joseph O'Donoghue, a Mercy College sociology professor who conducted the survey. The companies, he said, would rather keep major heists quiet than punish suspected offenders and risk publicity about lax security.

O'Donoghue warns that this perception could lead to "four or five people pulling a billion-dollar heist. It's merely a matter of knowing how the terminal works."

Public Phone Secrecy

Regional Weekly News

New Jersey Bell has imposed a veil of secrecy on the locations of its public phones, fearing that publicizing that information would unduly expose them to vandalism.

Hanover's Township Committee was required to pass a resolution at a recent meeting, agreeing to such non-disclosure as a condition for installing its 911 emergency dialing system.

After the measure was approved, a non-plussed Mayor Sal Iannaccone asked a reporter in the audience, "Can you believe that they won't let us tell people where the public phones are?"

Capitol Hill Hacker

The New York Times

Jennifer Kuiper was working late at her computer terminal in the office of Representative Ed Zschau of California on March 7 when she heard a beep that told her someone had entered the computer system from an outside telephone line. Twenty minutes later, her computer screen went blank. When service was restored, copies of more than 200 letters sent to constituents and information on mailing addresses had disappeared.

Four days later, staff workers for Representative John McCain of Arizona told the police they had discovered that someone outside their office had reached into McCain's computer and destroyed hundreds of letters and mailing addresses over the lunch hour.

Both of these representatives are Republicans and both are seeking Senate seats this November. These were apparently the first computer break-ins on Capitol Hill, where computers are increasingly being used, especially for record-keeping and answering mail.

"Every office on Capitol Hill can be broken into in this way and the files deleted. It can bring the work that a member of Congress does to a complete halt," said Zschau. [We had no idea it was this easy to grind the government to a halt, folks.]

Stephen A. Armstrong, vice president of Micro Research, the company that provides computers and related equipment to more than 150 members of Congress, including these two, said that whoever broke into the computers "would have to have a password and two security codes to get in."

Citibank Money Games

The New York Times

"You added funds...November 13...$60,000,050.00"

If you have ever dreamed of opening your monthly banking statement to find a transaction like that, you can probably feel the excitement Nelson Nash felt when he did just that. You can also feel his heart breaking when he read down a few lines more. On the very same day, Citibank recorded a withdrawal of $60,000,050.00.

"I usually check my balance every day or two," he said. "If I had been in town and seen that I had $60 million, I would have taken the money in unmarked bills and escaped!"

But a Citibank spokesman countered, "Even had it been on his record for several hours, and had he checked his balance and run to his branch, it would not have been given to him. It would have been questioned. People don't keep $60 million in their checking accounts."

[But keep an eye on your *savings* account balances!]

LETTERS OF THE MONTH

Dear *2600*:

Can any of your good phone phreak readers who are willing to explore the British telephone system contact me at my address in London? If you wanted to make a long distance call in London, you could call the operator, and BS her and she might just put your call through for nothing. This method only works if you get through to a happy operator. When phoning the international operator in London, he or she asks for your number and the international number. The operators in our country are very stupid. You could BS them all day long and they would think that the call they received is a true call, not a false call. Our international operator can be reached by phoning an inward for London and 01155 is the number which can reach her.

Another thing I like doing is what you folks over there call scanning. I spent hours scanning phone lines for interesting things and I only came up with one number: 200020. After the last digit has finished, depress the hookswitch (the thing that you rest your telephone on). Depress it for half a second, then bring it up again. You should hear the central office switching you through to this weird number. Keep listening to the phone line and after about 20 seconds you will hear a one second tone burst. I don't know what to do after that.

The cellular telephone system is good in our country, but I haven't had time to explore it. The number for it is 010836 (that includes the London dialing code—the first 0 is not needed when outside England).

Twilight Zone The Phreaker
12 Barn Way, Wembley Park, Middlesex HA9 9NW
London, England

Dear *2600*:

In response to police "sting" BBS's, why not get one of those books that list stolen and expired credit cards (they are issued weekly or bi-weekly). Type the contents into a disk and dump 40 megabytes of burned credit card numbers into these cop traps to spring them safely. If it comes to trial, tell the jury where you got them and watch the DA blush and the jury laugh. If the cops had any sense, that is what they would dump into any system collecting credit card numbers.

JN
Illinois

Dear JN:

Good idea, but how many of us are willing to go through with the expense and embarrassment of being hauled into a court of law just to make a DA blush? And what happens if the jury has no sense of humor? Since we're not especially fond of credit card fraud, we have no objection to people posting whatever numbers come into their heads or even random computer-generated numbers. That way, the criminals are confused, the authorities are confused, and democracy is safe for a little while longer.

Dear *2600*:

In the December 1984 issue of *2600*, you mention in the article on the "Scariest Number in the World" that the phreak recognized that the number was non-suped, using a technique that "experienced phreaks know". I'd like to consider myself an experienced phreak. How do I tell?

Don't say, "Just try calling it from a pay phone" because all long distance non-suped numbers won't go through without paying (the damned TSPS payphone console won't respond to reason). Local non-suped numbers work though (for the payphone repair).

Another method is by calling and if it doesn't appear on your next bill it ain't suped. This has several drawbacks, cause if it is, well then, I've got a one minute call to Australia on my bill. Also, waiting a month to find out ain't that expedient.

Lord Peter Wimsey

Dear LPW:

These days, this point is open to debate. Many phone phreaks can hear all kinds of little sounds that tell them things the average person doesn't even think about. One phreak we know can tell whenever a phone call is routed through Florida just by the sounds he hears! Some phreaks also claim they can tell if a call is supervised (i.e., registered on the billing computer) by the sounds that are made when the called party picks up. Generally, if no click is heard when they pick up or when a recording comes on, the call is thought to be "non-suped" or free. But exceptions abound. For one thing, many new electronic switches (Northern Telecom's DMS-100, for one) barely make any noise when they are picked up. If you were to call someone who had one of those, you might mistakenly think the call wasn't supervised. Then there are alternate long distance companies that have been known to charge people for calls that were never completed. Some companies aren't able (or willing) to recognize that a busy signal or a ring is different from the merry chimes of human speech.

And not only are non-suped numbers not always free, but free numbers aren't always non-suped! Take 800 numbers—they do *show up on a billing computer somewhere in many cases. You're simply not billed for them.*

An operator is usually able to tell you if the call you are placing is billable—but the operator has to place the call to find this out! This can be a challenge, to say the very least.

Dear *2600*:

What happened to the 2600 phone book?

How well is your mailing list protected against seizure by authorities?

Dr. William Wainwright

Dear WW:

There is a small phone guide (the 2600 *Phun Book) in existence that is available on many BBS's, The Private Sector (2013664431) included. You can also get a copy through our reader bulletin board, which is up Friday and Saturday nights, from midnight to noon, Eastern time at our office number (5167512600). Many of these numbers have already been printed in our issues, but if you want a full printout of the 400 or so interesting numbers, send us $2.50. By the way, we always need more numbers, so please send us what you've got.*

Our mailing list is only seen by Twenty Six Hundred. It will not be sold, lent to, seen, or turned over to anyone. That is our policy. We don't believe the authorities pose any threat in that department, especially since so many different kinds of people read this magazine.

Dear *2600*:

I would like to take this time to thank you for your commendable work. It's people like you that make me proud to say I'm an American. I wanted to get this message to you as soon as possible. I represent only a small part of the large world of computer antics, which consists of phreakers, hackers, and piraters. Upon the receipt of this message, please discard (a small atom bomb will do the trick) and forget ever receiving it. Thank you.

John Smith Hacker

Dear JSH:

Don't worry. It has been destroyed.

(continued on page 3-48)

The 2600 Information Bureau

800-342-1143	800 OPERATOR	800-323-2005	CARRIER
800-342-1119	LOUD TONE	800-323-3107	CARRIER
800-368-1017	TEST #	800-323-1146	CARRIER-LIKE SOUNDS
800-368-1018	TEST #	800-323-4279	CARRIER
800-621-4562	?????	800-323-4297	ASKS FOR 7 DIGIT ACCESS CODE
800-527-2007	300 BAUD	800-323-1151	LD DIVERTER
800-527-2551	CARRIER	800-323-4313	PBX
800-343-2903	CALL AMERICA LDS	800-323-4376	CARRIER
800-527-2011	CREDIT AUTHORIZATION	800-323-4377	CARRIER
800-368-1040	ATT INFO SYSTEMS	800-323-4462	CARRIER
800-221-2000	TWA RESERVATIONS	800-323-8021	TRY THIS!
800-221-2014	EXTENDER	800-323-8039	PBX
800-424-5900	PBX	800-323-4298	SPECIAL OPERATORS
800-424-6200	ODD SERVICE	800-323-4354	SPECIAL OPERATORS
800-343-6400	PBX WITH RECORDING	800-526-2000	"YOU'VE GOT EQUIPMENT PROBLEMS?"
800-221-9735	CARRIER	800-342-1105	TONE
800-221-7210	BANK OF NY	800-342-1108	TONE

SPECIAL AT&T SERVICES

800-331-1323 DIRECT CONNECTION TO FRENCH OPERATORS!! [WE THANK THE MANY READERS WHO SUPPLIED US WITH THIS NUMBER AFTER WE REQUESTED IT LAST MONTH.]

800-222-0300 AT&T TOLL-FREE WAKE-UP SERVICE. YOU ARE LULLED TO SLEEP BY THE PEACEFUL SOUNDS OF GEORGE WINSTON AT PIANO AND AWAKENED BY YOUR PLEASANT AT&T REPRESENTATIVE IN THE MORNING. (CALL LATE AT NIGHT AND IGNORE INITIAL VOICE MESSAGES.)

800-555-8111 AT&T ALTERNATE TOLL-FREE WAKE-UP SERVICE, FOR THOSE WHO PREFER TO LISTEN TO CHEERY MUZAC WHEN THEY FALL ASLEEP. AN AT&T REPRESENTATIVE WILL AWAKEN YOU IN THE MORNING. (CALL LATE AT NIGHT AND IGNORE INTIAL VOICE MESSAGES.)

2600 (ISSN 0749-3851)

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley David Ruderman

Executive Director
Helen Victory

BBS Operator
Tom Blich

Cartoonist
Dan Holder

Junk Mail Receiver
Richard Petrovich

Writers: Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

2600 is published by 2600 Enterprises, Inc., an eleemosynary organization.
ANNUAL SUBSCRIPTION RATES: $12, individual; $30, corporate; $20, overseas.
LIFETIME SUBSCRIPTION: $260. SPONSORSHIP: $2600.
BACK ISSUES: $2 each, individual; $3 each, corporate; $2.50 each, overseas.
MAKE CHECKS PAYABLE TO: 2600 Enterprises, Inc.
WRITE TO: *2600*, P.O. Box 752, Middle Island, NY 11953-0752.
TELEPHONE: (516) 751-2600. PRIVATE SECTOR BBS: (201) 366-4431.
ADVERTISING DEPARTMENT: P.O. Box 762, Middle Island, NY 11953-0762. Call for rates.
ARTICLE SUBMISSION AND LETTERS: P.O. Box 99, Middle Island, NY 11953-0099. We readily accept articles, letters, clippings, artwork, and data for publication.
POSTMASTER: This is private mail.

Nobody knew why old Mr. Ferguson suddenly got a $25,000 phone bill.

Groups Concerned with Computer Security, Computer Ethics, and Certification of Computer Professionals:

American Bar Association Task Force on Computer Crime, 1800 M. St. NW, Washington, DC 20036.
American Institute of Certified Public Accountants, 1211 Avenue of the Americas, NY 10036 (212) 575-6200.
American Society for Industrial Security, National Computer Security Committee, 1655 N. Ft. Myer Dr., Suite 1200, Arlington, VA 22209 (703) 522-5800.
Association for Computing Machinery, Special Interest Group on Security Audit and Control, Special Interest Group on Computers and Society, 11 W. 42 St., NY 10036 (212) 869-7440.
Bank Administration Institute, 60 Gould Center, 2550 Golf Road, Rolling Meadows, IL 60008 (312) 228-6200.
Boston Computer Society, Social Impact Group, 1 Center Plaza, Boston, MA 02108 (617) 367-8080.
Computer Professionals for Social Responsibility, P.O. Box 717, Palo Alto, CA 94301 (415) 322-3778.
Computer Security Institute, 43 Boston Post Road, Northborough, MA 01532 (617) 845-5050.
Data Entry Management Association, P.O. Box 16711, Stamford, CT 06905 (203) 967-3500.
EDP Auditors Association, 373 Schmale Road, Carol Stream, IL 60187 (312) 682-1200.
IEEE Social Impact Group, c/o F.A. Furfari, 117 Washington Rd., Pittsburgh, PA 15221
Information System Security Association, P.O. Box 71926, Los Angeles, CA 90071 (213) 480-5516.
Institute for Certification of Computer Professionals, 35 E. Wacker Dr., Chicago, IL 60601 (312) 782-9437.
Institute of Internal Auditors, 249 Maitland Ave., Box 1119, Altamonte Springs, FL 32701 (305) 830-7600.
National Center for Computer Crime Data, 2700 N. Cahuenga Blvd., Los Angeles, CA 90068 (213) 850-0509.

Publications Concerned with Computer Ethics, Computer Security, Computer Crime:

Computer Control Quarterly, 26 Washington Ave., East Malvern, Victoria 3145 Australia (03) 211-3737.
Computer Fraud and Security Bulletin, Elsevier International Bulletins, 52 Vanderbilt Ave., NY 10017.
Computer Crime Digest, 70432 Wimsatt Road, Springfield, VA 22151-4070 (703) 941-6600.
Computers and Security, Elsevier International Bulletins, 52 Vanderbilt Ave., NY 10017.
Computers and Society, c/o Richard Rosenberg, Department of Mathematics, Statistics and Computing Science, Dalhousie University, Halifax N.S., Canada B3H 3J5.
Computer Security, Computer Security Institute, 45 Boston Post Road, Northborough, MA 01532 (617) 845-5050.
Computer Security Alert, 500 N. E. Spanish River Blvd., # 8, Boca Raton, FL 33431 (305) 392-5411.
Computer Security Digest, 711 W. Ann Arbor Trail, Suite 4, Plymouth, MI 48170 (313) 459-8787.
Conscience in Computing, 2700 N. Cahuenga Blvd., #2113, Los Angeles, CA 90068 (213) 850-0509.
Data Processing Auditing Report, Box 85, Middleville, NJ 07855 (201) 383-3928.
EDPACS Automation Training Center, Inc., 11250 Roger Bacon Dr., Suite 17, Reston, VA 22090 (703) 471-5751
Information Security Monitor, Durrant House, 8 Herbal Hill, London EC1R 5JB England (01) 278-3143.
Personal Identification News, P.O. Box 11018, Washington, DC 20008.
Privacy Journal, P.O. Box 8844, Washington, DC 20003 (202) 547-2865.
Processed World, 55 Sutter St., #829, San Francisco, CA 94104.
Reset, c/o Mike McCullough, 90 E. 7th St., NY 10009.
Security Audit and Control Review, c/o ACM, 11 W. 42 St., NY 10036.
2600 Box 752, Middle Island, NY 11953.

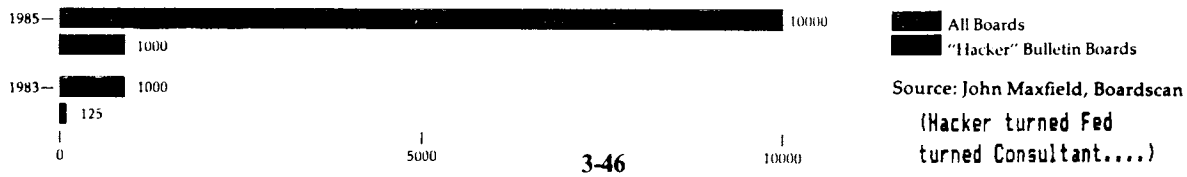
Sources of Information about Computer Ethics Courses:

Joan Abrams, Superintendent of Schools, Public Schools of Red Bank, New Jersey, Administration Building, 76 Branch Ave., Red Bank, NJ 07701 (201) 842-4954.
Robert Cogan, Edinboro University, Department of Philosophy, Edinboro, PA 16444 (814) 732-2490.
Kay Gilliland, Equals Project, Lawrence Hall of Science, University of California, Berkeley, CA 94720 (415) 642-1823.
Montgomery County Public Schools, Rockville, MD
John Snapper, Illinois Institute of Technology, Chicago, IL 60616 (312) 567-3017.

Consultants and Researchers Providing Information for this Report:

Kevin Fitzgerald, 26 Washington Ave., East Malvern, Victoria 3145 Australia (03) 211-3737.
John Maxfield, Boardscan, 19815 W. McNichols, Detroit, MI 48219 (313) 534-1466.
Donn Parker, SRI International, 333 Ravenswood Ave., Menlo Park, CA 94025 (415) 859-2378.
Erdwin H. Pfuhl Jr., Department of Sociology, Arizona State University (602) 965-6311.
Dr. Ulrich Sieber, Innsbrucker Strasse, 22 7800 Freiburg I.Brsg., West Germany 07 61 44 14 66.
Arthur Solarz, Swedish National Council for Crime Prevention, Atlasmuren 1 S-113 21, Stockholm, Sweden 08-22 97 80.
Dr. Ken Wong, BIS Applied Systems Ltd., Maybrook House, Blackfriars St., Manchester M3 2EG England 061 831-0731.

Chart 258: Bulletin Boards



(Hacker turned Fed turned Consultant....)

SYSTEMATICALLY SPEAKING

Hands Across Telenet

The New York Times

In order to accomplish Hands Across America last month, first a nationwide network of technology had to be formed to coordinate the event.

In their attempt to combat hunger, Hands Across America organized millions of people to donate money, buy T-shirts, and hold hands.

"Three or four years ago this event could not have been done," said Fred S. Droz, the national project director of Hands Across America. "Computers, TV, telephones, teleconferencing—the technology has to come together."

The logistics of keeping track of millions of people and the millions of dollars they have pledged would have been overwhelming without computer power and communications networks, which permit the gathering, storage, and transmission of information. The process required staggering amounts of data—names and addresses, route assignments, directions, amounts of donations and credit card numbers, to name but a few. In addition organizers had to keep track of details such as local permits, water supplies, and the availability of medical facilities.

As a result of the Hands project, they have developed a database system that has the potential to control future nationwide fund-raising campaigns with pinpoint accuracy.

GTE Telenet Communications donated its 237,000 miles of computer network and overseas satellite hookups to the Hands project. Over this network, a wide variety of computers can send information back and forth at high speed.

The Source, an information system, joined with GTE to offer its 60,000 members free computer access to information about the Hands project.

Kiev Calling Clogged

Newark Star Ledger

In the wake of the recent nuclear plant accident in Chernobyl, the volume of telephone calls being made to the Soviet Union has tripled, a spokesman for AT&T International said.

All calls from the United States to the Soviet Union are routed through the AT&T International Operation Center in Pittsburgh. "All these calls have to go through operators in the Soviet Union. A lot of times we'll have a lot of attempts, but not completions," said Rick Brayall of AT&T-I.

AT&T no longer has direct-dial service to the Soviet Union. Because of the unusual volume, callers must wait several hours on reservations for calls to Moscow and Kiev.

AT&T cannot employ any more personnel to put the calls through, because "there is no point in having 50 American operators trying to get calls through to only two Soviet operators," Brayall said.

Nynex Bumps Southwestern Bell

Combined News Sources

"A clerical error," caused the omission of Southwestern Bell's New York office number from the latest edition of the Nynex Manhattan Yellow Pages.

Southwestern Bell of St. Louis planned to publish its own Manhattan Yellow Pages directory that would compete directly with Nynex.

In total, three listings for Southwestern Bell were "accidentally" dropped: its Yellow Pages; Ad-Vent, a graphics operation; and the Silver Pages, a national directory for the elderly.

"If advertisers can't find us in the (Nynex) Yellow Pages, they will figure we aren't a viable entity," complained Al C. Parsons, president and chief executive of Southwestern's publishing arm which still intends to publish its "Clone Book" this fall. "It's sure awfully convenient for this to happen now," he noted.

Stock Market Crash

InfoWorld

Options trading on the London Stock Exchange ceased for a day recently following the crash of a new electronic trading system. The crash has cast a pall over the Stock Exchange's Automated Quotes system, which will be used for share trading after the October deregulation of financial services in London.

The failed system consists of five IBM PC AT's linked together by a network, with an additional AT as network controller.

"Ed Quinn Cell Site"

USA Today

Bell Atlantic Corporation's cellular telephone division has been rewarding top employees by naming a cell site after them.

A plaque bearing the employee's name adorns the site, which is usually little more than an antenna tower next to a garage-sized building housing a cellular phone relay.

Two employees a month will be recognized, which means that Bell Atlantic has two years worth of honors to dole out and more sites are being built every day. So far there's Susan Schuhalter cell site, Kathy Schaefer cell site, and Ed Quinn cell site. Winners get to choose their own site.

Let's Move To France!

The New York Times

In Biarritz, France, people dial "01-28-62" to reach the world's only "televideoclub," that offers each subscriber a choice of more than 2,000 video cassettes to look at on their video-phone, a combination television and telephone.

This summer, an estimated 1,500 Biarritz houses will be equipped with the tabletop machine that incorporates a television screen and a movable video camera. They will be hooked to an underground web of optical fibers that can carry 10 times the amount of information as a normal coaxial cable.

This project was started three years ago by President Mitterrand and provides for the wiring of all major French towns and cities by the end of the century while at the same time establishing France as the world leader in this technology. By the end of 1988, 3.1 million homes are expected to be connected to optical fiber systems.

In Biarritz, videophone owners can see each other as they chat and can walk around with a hand-held camera transmitting pictures to a friend.

They can dial into Televideoclub, request a film and watch it on their home screen. Or they can choose among 12 television channels and can switch to larger screens elsewhere in their homes, or select one of six stereo radio stations. Or they can plug into visual data banks and sift huge amounts of information, from train schedules to the latest stock market prices. At the local hospital, doctors can call up patients' medical records and X-rays on a videophone during consultations and sick children can follow classes in the local school from home.

Biarritz also has several pay videophones in kiosks on the street.

At present, a single videophone costs $3,000 and is expected to fall to $800 for a town of 300,000 houses.

Watching an hour-and-half-long film on video cassette now costs about $5.

LETTERS

(continued from page 3-44)

Dear *2600*:

Enjoyed your article on mobile phones (April 1986)—reminds me of the old *TAP* which I miss. One comment though on the end of that article where you refer to the FCC catching up. In my area we have three engineers for a many state area and they cover ham radio, CB no more, broadcast, public safety, microwaves, etc.—get the idea? They won't bother you without a lot of complaints. The ones to look out for are the phone company's goon squad. Be careful but don't sweat the FCC for a few tests—do watch for the phone company who is very sensitive to any disruption of their revenue.

Seagull

Dear *2600*:

How can I be like Captain Midnight? How about an AM carrier-current pirate radio station?

PV

Dear PV:

We can't tell you what to do exactly, but we can say that it involves ingenuity, sneakiness, intelligence, persistence, and a youthful spirit. Mix those together and you should come up with something worthwhile.

There are many AM carrier-current pirate radio stations in existence. Too many of them try to sound like regular AM stations and few people notice anything different.

Dear *2600*:

Your *2600* magazine is great! I really enjoy it. Your article on mobile phones was most interesting. I'm very interested in this area, and look forward to any future articles on it—such as what make and model of two-way radio is best (and cheapest) to use, or what radio is best (and cheapest) to just listen in on calls.

Dear *2600*:

I have something interesting to report about RCI. RCI is another one of the long-distance telephone companies. They use optical fiber networks that have been laid along railroad tracks around the country. If you are near where their cables run, there is a sign that tells you what to do if you wish to dig the cables up. The signs give a location which is the initials of the state you are in and a number which is usually less than 1000. You simply call 8003279686 and you get an RCI operator who may chat with you for hours about cable sites around the country.

She can give you cable locations, and she might want to know if you plan on digging a few cables up.

Right Track

Dear Readers:

Yes, it finally happened. We lost track ourselves of the difference between Flash and Systematically Speaking and accidentally mixed them up last month. We regret the error.