discourse" and chatter about rap music instead? Be patient, counsel the math wizards.

"I tell people over and over: Don't expect it to happen overnight," says Shirley Hill, former chair of MSEB and professor of math and education at the University of Missouri. "Kids are conditioned otherwise and they're not going to expect math to be fun or relevant all of a sudden. It's a process." The best math teachers already run classrooms like those in the standards, says Carl.

For reform to spread, educators say it's important that all these projects—and many smaller ones not mentioned here—work together, or at least pull in the same direction. "No one will succeed in isolation," says Williams. But while there's much agreement on what teachers should strive for, each program has a slightly different vision of the future. It's not exactly clear, for example, how the new math standards fit with "Science for All Americans," which includes math, but less of it.

And new programs are coming. The National Academy of Sciences, for example, is expected to decide upon a much-expanded role for itself in science education in late December. A few educators who work for existing programs fear the academy will repeat or compete with their efforts, although executive officer Philip Smith insists the institution won't invade any turf. Academy officials are still plotting their strategy and Smith defers any detailed revelations until later this month. But he says they're considering a two-pronged approach, to provide immediate relief as well as long-term vision. And he hints that the academy may tackle undergraduate instruction, an arena where other educators say they'd especially welcome the academy's clout.

For the moment, all sides tend to downplay whatever differences may exist. "It doesn't hurt at all to have different experiments going on simultaneously," says Susan Snyder of NSF's division of teacher preparation and enhancement. "We'll probably never have one single answer."

Snyder and other educators would prefer to focus instead on the momentum for change. The president and National Governors' Association, they boast, have announced the goal of having U.S. students first in math and science by 2000. Privately, though, almost no one thinks that can be done. At least, those involved plaintively conclude, the goal is on the national agenda. The unspoken question: How long will our easily distracted society keep it there? Back in Wisconsin, Joel Marino had the perseverance to complete his model of a mid-ocean ridge with chicken wire, blue plastic, kitty litter, and a mysterious red substance that quickly developed fruit flies. If the education experts succeed equally well with their own models, then Joel—or at least his younger siblings—may one day admit that science and recreation can sometimes be the same thing. ■ ELIZABETH CULOTTA

*Elizabeth Culotta is a science writer for the* Milwaukee Journal.

# Computer Security: NAS Sounds the Alarm

Electronic vandals, viruses, and other malignancies of the computer world are likely to grow more virulent soon, according to a new report from the National Research Council. Indeed, a panel of computer security experts chaired by David Clark of the Massachusetts Institute of Technology warns that unless preventive action is taken, the economy could suffer. In a study titled "Computers at Risk," the panel calls for the establishment of an Information Security Foundation, a private nonprofit body that would set standards, promote research, and review the "trustworthiness" of computer software and hardware. It would require federal support to get started, says one panel member, and after that, it could support itself with membership dues.

"To date, we have been remarkably lucky," the report begins. Money has been stolen by computer—perhaps millions of dollars from credit card companies alone—and "lives have been lost because of computer software errors." But no intruder has been able to "subvert" a critical system. Yet the report warns that "there is reason to believe that our luck will soon run out."

The reason: Little is being done outside the government to reduce the vulnerability of computer networks, even though the nation's reliance on them is growing. For example, no concerted effort has been made to plug the many faults of personal computers, which are difficult to make secure because of the way they were designed. As network linkages grow, more PCs will be connected, and the weak points in systems will increase. "There's no doubt that things get considerably more dangerous when you get unprofessionally administered machines on networks," says panel member M. Douglas McIlroy of AT&T Bell Laboratories.

Most computer and software manufacturers have failed to take the risks of attack seriously, responding to problems as they occur in an "episodic and fragmented" fashion, says the report. And within government, computer security work is concentrated in the National Security Agency, which has been constrained by its secrecy and its national defense mission.

However, McIlroy points out that between 1983 and 1990, the NSA ran an advisory body "outside the perimeter" of secrecy called the National Computer Security Center. It set public standards and served as a clearinghouse for research. This was a valuable service for the handful of companies—like his own AT&T—that wanted to develop better defenses. But this year, the NCSC went back "behind the wire" of secrecy, McIlroy says, and it's not clear that any other office will step in to serve the public. The National Institute of Standards and Technology (NIST) might fit the bill, but the report comments that NIST "has limited technical expertise and funds" to do the work. Congress gave it only $2.5 million for computer security programs in 1990; when NIST attempted to double this budget for 1991, the increase was axed by Congress.

Meanwhile, companies are reluctant to advertise security problems. Their customers often aren't convinced that they're real. Unless they have been stung themselves, says McIlroy, they may not want to bear the costs of improving systems. Many computer users try to get around the problem in a superficial way, using security gimmicks of one kind or another. As a result, hundreds of products are offered for sale, but there's no objective means of judging their quality. The Clark report recommends several actions, in addition to creating a new foundation:

- Establish guidelines for "trustworthy systems" that reflect the consensus of security experts.
- Take a series of immediate short-term actions such as creating emergency response teams and asking vendors to ship products with security systems automatically turned "on."
- Create a system to monitor security breaks and to collect data on them for research.
- Clarify a confusing jumble of export controls and consider relaxing limits on the use of the U.S. Data Encryption Standard.
- Develop and fund a comprehensive program of research on computer security issues. ■ ELIOT MARSHALL