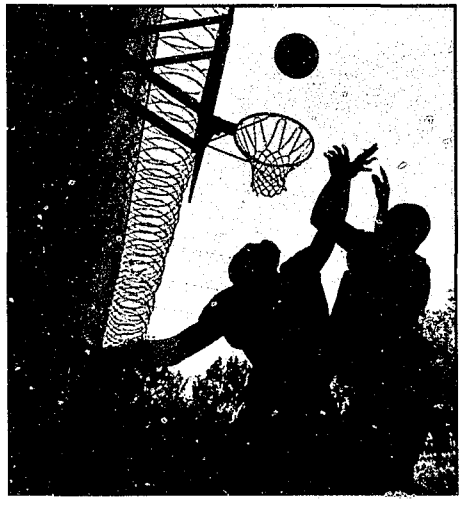
Make your
ters
your
ution—
from
abuses

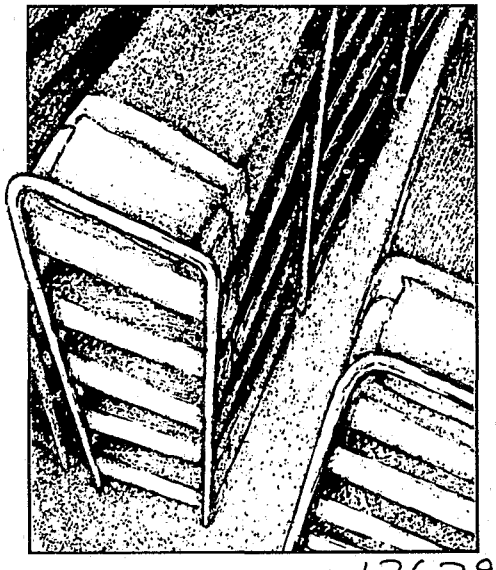
es and Computers

in...

Contents

VOL. 1, NO. 2 ■ FALL 1989





Inmates and Computers

Managing access, preventing abuse

Christopher Erlewine and Helene Cavior

Computer crime is a fast-growing category in the national crime statistics, but isn't confined to "the streets" or "the suites," as these stories illustrate:

■ An inmate assigned to work on a personal computer in the business office in a prison industries operation was also taking computer courses in the education department. Relying on his expertise, staff used the inmate to load software on their personal computers. One day, a search of his housing quarters yielded a significant amount of computer-related documentation, including correspondence with a female acquaintance who worked for a California computer products manufacturer. The correspondence indicated she had been sending computer chips and modems addressed to the inmate as if he were an employee in the prison industries department.

The FBI made a test call to the company in California. They discovered company employees were on a first-name basis with the inmate, apparently believing he was a member of the prison staff. A subsequent search of the inmate's work area and classroom area yielded a variety of contraband hardware.

■ Staff at a State department of corrections discovered that someone was trying to access their computer system to change the sentencing information of a State inmate who was boarding at a Federal Correctional Institution and working on a computer job assignment. State law enforcement officials traced the computer access attempts back through the telephone lines to the Federal Correctional Institution where the State inmate was located, but were unable to link the inmate conclusively to the file-tampering attempt.

The inmate was transferred to another Federal prison, where he was perceived to be a soft-spoken, computer-knowledgeable, helpful employee. He was given a job in the recreation department in a room with a computer. Whenever the inmate was left alone in the room, the staff disconnected and locked up the telephone, but the inmate still had access to the phone lines. A subsequent search of the inmate's floppy diskettes and the hard drive on his computer revealed unauthorized homemade programs designed to give him access through the phone lines to other electronic devices. The inmate was reassigned to a job where he would not have access to a computer.

■ An inmate near release developed a program for staff use that self-destructed several weeks following his release. All that remained on the computer screen was a message with his name and address and the suggestion that he would be happy to help the institution get back on line "for a price."

A new security problem

Like the rest of society, prisons increasingly rely on personal computers. Effective use of this new and rapidly changing technology requires significant computer knowledge; however, most prison staff are not computer-literate. The computer expertise vacuum among staff at many Federal prisons is all too often filled by inmates.

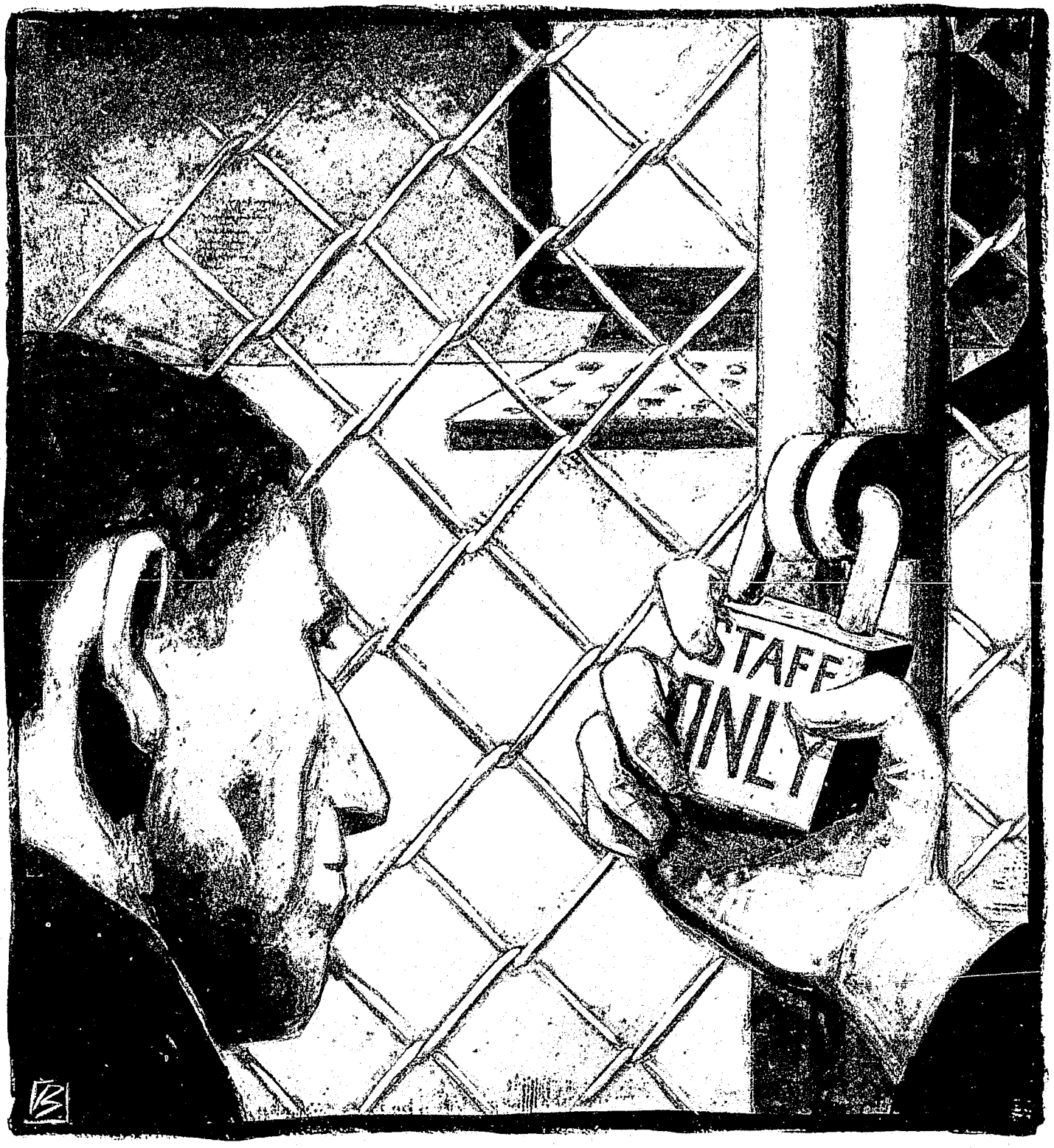
Some inmates acquire computer skills prior to incarceration, but many learn about computers in vocational training classes, on their job assignments, or through self-study during their leisure time. Inmates with computer skills volunteer to write programs that improve job productivity. The result for the institution is an entirely new security concern: dependence on inmate computer expertise.

While staff sincerely want to use personal computer technology to carry out their responsibilities more effectively, training time is limited and few have the necessary skills. Thus they turn to the only skilled source available—the inmates. Due to the low level of staff computer expertise, those responsible for supervising inmate employees often cannot use the computer programs these employees create. In many cases, staff cannot detect that inmates are misusing computers even though they often maintain direct visual observation of, and work in the same room with, the inmate computer operators.

One way to curtail inmate computer abuse is to ban all inmates from using computers. Although this sounds like a simple solution, additional staff positions would be needed to replace the inmate operators, and useful work and educational opportunities for inmates would be lost.

As a result of the security breaches that have occurred due to inmate computer use, the Federal Bureau of Prisons established a task force to determine if effective security measures could be taken short of banning all inmates from using computers. A careful review of inmate-related computer security violations found several categories of abuse:

• *Overdependence on inmate computer programmers and operators.* Staff have permitted inmates to develop programs, used to conduct the work of the institution, in which the inmate programmers controlled passwords and access codes—and therefore staff access. In one



Tim Bower

instance, where staff appeared to control access to the program, the inmate programmer had created a system of hidden files and designed the program to malfunction periodically. As a result, staff became dependent on his computer skills; by allowing him to repair the program, they gave him continued access to these hidden files. Some inmate programmers attempt to foster such dependence and then use it to seek favors or avoid disciplinary action (e.g., how can inmate X be placed in disciplinary housing when he is the only person who can keep the department's programs functioning?).

■ *Inmates have been given too much computer access.* On more than one occasion staff have allowed inmates to operate computers with modems, thereby facilitating unmonitored communication via telephone lines.

Staff want to keep their inmate employees happy, particularly those possessing the computer skills on which they depend. Consequently, they may purchase powerful utility programs based only on the inmate's assurance that such software is needed to carry out work-related tasks more efficiently. These utilities are often used by the inmate to create hidden files, which further limits the effectiveness of staff surveillance.

■ *Inmates misuse computer equipment.* Inmates have attempted to use personal computers and modems for unmonitored communications with their cronies in the community. At one institution, inmates constructed contraband modems while working in a personal computer vocational training program. At other institutions, inmates have arranged for family or friends to smuggle in contraband modems.

By demonstrating even a little computer knowledge, inmates often convince computer-illiterate staff that they possess significant programming skills.

Inmates have used computers to store information pertaining to escape attempts and other illegal activities. At a Federal penitentiary, inmates used a computer in the education department to plan a helicopter escape involving members of three domestic terrorist groups. A contraband modem was located near the computer, and the hard drive containing hidden files related to the escape was seized by the FBI.

■ *Inmate programmers often lack computer skills.* By demonstrating even a little computer knowledge, inmates often convince computer-illiterate staff that they possess significant programming skills. In reality, the programs they create are often amateurish and poorly constructed. Without other reliable sources of computer expertise, however, staff feel they have little option but to rely on inmates.

Eliminating dependence, strengthening security

After studying the problem for several months, visiting several field sites, and surveying all Federal institutions, the task force developed a series of recommendations to eliminate staff dependence on inmate computer expertise and to provide more controls and safeguards on computers to which inmates are permitted access:

■ *Give staff reliable computer support by establishing a full-time computer specialist position at every institution.* A computer specialist will provide staff with *a* reliable source of information. The computer specialist will serve as the institution's computer security officer and implement an effective security program by heading an institution computer security committee, auditing computer usage and security measures, providing computer training and technical support, and documenting and assisting in local program development.

The computer specialist will provide training in how to use commercial software and specially developed applications. In addition to being able to provide cost-effective onsite training, the specialist will also perform preventive maintenance and troubleshoot hardware problems.

The computer specialist will maintain and document locally developed software applications. Programs developed by institution staff often fall into disuse after the developer transfers out of the institution because his or her replacement does not know the program exists or how to use it. The continuity provided by the computer specialist will eliminate this problem.

■ *Prohibit inmates from writing programs that are used to conduct the work of an institution.* As long as inmates are allowed to write personal computer programs, they are in a position to ask for favors; they can include routines in the program that do things staff don't know about; they can design programs to fail at specified intervals, increasing staff dependence on their expertise and providing the inmates with access to

program data; they can set up passwords to deny staff access; and they can do things we haven't even thought of yet.

The benefits of allowing inmates to write programs—meaningful personal computer work for inmates in vocational training programs and on the job—do not seem to outweigh the security risks involved.

Staff supervision of inmate programming has been insufficient to guarantee that abuses do not occur. To effectively monitor and supervise the work of an inmate programmer, staff need to have equivalent or superior programming skills. For effective security, staff programmers need to create the programs used in prisons.

■ *Standardize prison personal computer programs with broad applications.* To maximize their effectiveness and reliability, programs with broad applications, such as those used to monitor visiting room activity, should be created, or at least carefully reviewed, by staff programmers at the headquarters level (such as the Bureau of Prisons' Office of Information Systems) This allows global updates and uniform documentation.

■ *Establish an institution computer security committee.* An institution-wide personal computer security program is essential to the success of each department's security efforts. Virtually any piece of software or hardware can be used in any personal computer. Consequently, a lapse in one department's security procedures can undermine effective controls in another department.

The computer security committee, chaired by the computer specialist and composed of institution staff with computer-related responsibilities, should develop and implement an institution-wide computer security plan.

The benefits of allowing inmates to write programs—meaningful personal computer work for inmates—do not seem to outweigh the security risks involved.

■ *Distinguish between personal computers used solely by staff and personal computers to which inmates have access and clearly label each machine as either "staff only" or "staff/inmate access."* Inmates will have no access to staff-only computers. As discussed below, there will be stringent controls on both the software and hardware on the computers to which inmates are permitted access.

■ *Limit inmate access to software through a combination of software and hardware security measures.* Staff/inmate-access personal computers will be configured to limit inmates to only the software needed for the specific task to be performed. Inmates will be prohibited from access to communications software and software that can be used to permanently erase, modify, or hide files. These constraints can be achieved with a combination of commercially available software security programs and hardware security devices. The security software controls access to programs, files, and directories through user ID's, passwords, file encryption, and assigned access rights. Hardware locks are needed to prohibit circumvention of the software security measures through the floppy disk drive. Inmate use of computers will generally be limited to data entry, basic word processing, and vocational training. These security measures will ensure that only staff can change or add programs, or remove data by disk, tape, or modem transmission.

■ *Prevent inmates with sophisticated computer skills from working on or using computers.* Policy already restricts inmates with knowledge of gunsmithing or explosives from work assignments that would offer them an opportunity to apply their expertise to the detriment of the institution. This approach should be applied to inmates with sophisticated computer skills, particularly to those who enter prison with records of computer fraud or other computer-related crimes, or who misuse computers while in prison.

Prisons are in the computer age to stay. Like any other complex organization, correctional institutions will be increasingly dependent on computers for more aspects of their operations. This dependence, however, does not mean leaving security at the mercy of technologically sophisticated inmates (and all large correctional systems include many of those). This article has outlined a workable strategy for keeping data—and institutions—secure, while preserving the managerial value of computers to prisons and their educational value to inmates. As with any other aspect of institution security, however, this strategy will ultimately depend on the training and diligence of staff. ■

Christopher Erlewine is Deputy Assistant Director, Program Review Division, Federal Bureau of Prisons. He chaired the Bureau's Task Force on Inmate Access to Personal Computers. Helene Cavior is a Computer Specialist in the Bureau's Western Regional Office.