Consider, too, what will happen when procedural controls are strengthened to the point that technical penetration becomes the path of least resistance. Since many years are needed to make major security improvements to existing systems, a sudden explosion of technical crimes will be very difficult to counter.

Probably because the computer industry is still in its infancy, sufficient knowledge of computers to exploit technical flaws seems to be rare among the dishonest. (On the other hand, perhaps they are so clever that they are not detected.) But as knowledge of computers becomes more common, we cannot assume that only a few honest citizens will possess the requisite skills to commit a major crime. Given the low risk of getting caught and the potentially high payoff, sophisticated computer crime is likely to become more attractive in the future, especially if the non-technical avenues to crime are sufficiently restricted.

One of the primary arguments that computers cannot prevent most cases of abuse is based on the observation that computer crimes committed by insiders usually do not involve a violation of internal security controls: the perpetrator simply misuses information to which he or she normally has access during, the course of normal work responsibilities. Something akin to artificial intelligence would be required to detect such abuse automatically. But on closer inspection, we often find that people routinely gain access to more information than they need, either because the system's security controls do not provide adequately fine-grained protection or because implementing such protection within the architectural constraints of the system is too inconvenient or costly. The problem appears to be solely one of people, but it is exacerbated by a technical deficiency of the system. The technical solutions are not apparent because an organization's way of doing business is often influenced by the design (and limitations) of its computer system.

2.6 TECHNOLOGY IS OVERSOLD

There has long been the perception that true computer security can never be achieved in practice, so any effort is doomed to failure. This perception is due, in large part, to the bad press that a number of prominent government-funded secure computer development programs have received. The reasons for the supposed failure of these developments are varied:

- Programs originally intended for research have been wrongly criticized for not fulfilling needs of production systems.
- Vying for scarce funding, researchers and developers often promise more than they can deliver.
- Funding for the programs has been unpredictable, and requirements may change as the programs are shuffled among agencies. Often the requirements ultimately expressed are inconsistent with the original goals of the program, leading to unfortunate design compromises.
- Developments are often targeted to a specific model of computer or operating system, and inconsistent levels of funding have stretched out programs to the point where the original target system is technologically obsolete by the time the program is ready for implementation.

Whitmore, J.; Bensoussan, A.; Green, P.; Hunt, D.; Kobziar, A.; and Stern, J. 1973. “Design for Multics Security Enhancements.” ESD-TR-74-176. Hanscom AFB, Mass.: Air Force Electronic Systems Division. (Also available through National Technical Information Service, Springfield, Va., NTIS AD-A030801.)
A description of the enhancements incorporated into Multics to support mandatory security controls.