

to assume any liability due to a program malfunction, but was unwilling to share liability due to an error in the engineer's calculations.
The programmer's position in this situation is:
The engineer's position in this situation is:

11. A manager of a company that sells Web hosting services bought similar services from a competitor. She used her access to the competitor's computer to try to break the security system, identify other customers, and cause the system to crash. She used the service for a year and always paid her bills promptly.

12. A student programmer decided to write a virus program. Such programs usually spread automatically by making copies of themselves onto other users' media (like flash drives). The student wrote a program that caused the computer to ignore every fifth command entered by a user. The student took his program to the university computing lab and installed it on one of the computers. Before long, the virus had spread to hundreds of users.

If the virus program output the message "Have a nice day," then the student's action of infecting hundreds of users' flash drives was:
If the virus erased files, then the student's action of infecting hundreds of users' flash drives would have been:

If the virus program output the message "Have a nice day," then the student's action of infecting hundreds of users' flash drives was:
If the virus erased files, then the student's action of infecting hundreds of users' flash drives would have been:

behavior is unethical or even illegal. Proper ethical and legal training is vital to creating an informed and well-prepared system user.

> Detering Unethical and Illegal Behavior

There are three general causes of unethical and illegal behavior:

- **Ignorance:** Ignorance of the law is no excuse; however, ignorance of policy and procedure is. The first method of deterrence is education, which is accomplished by obtaining agreement to comply with these policies and relevant laws, and front of employees to support retention and compliance.
- **Accident:** People who have authorization and privileges to manage information within the organization are most likely to cause harm or damage by accident. Careful planning and control help prevent accidental modification to systems and data.
- **Intent:** Criminal or unethical intent goes to the state of mind of the person performing the act; it is often necessary to establish criminal intent to successfully prosecute offenders. Protecting a system against those with intent to cause harm or damage is best accomplished by means of technical controls, and vigorous litigation or prosecution if these controls fail.

Codes of Ethics of Professionals

Many professional organizations have codes of ethics that members are expected to follow. These codes of ethics are a level of certification or professional fear losing that accreditation or professional or accreditation can dramatically impact a professional's career. Security professionals have a responsibility to follow these codes of ethics.

- **Fear of penalty:** Penalties or verbal warnings or forfeiture of pay.
- **Probability of being caught:** Possibility of being caught.
- **Probability of penalty:** Probability of penalty will be administered.

Whatever the cause of the behavior, security professionals must have a value of policy. However, if three conditions are met, the behavior is unethical or even illegal.

Figure 3-6 Deterrents

