These concepts of information security also apply to the term *information security;* that is, internet users want to be assured that

1. they can trust the information they use
2. the information they are responsible for will be shared only in the manner that they expect
3. the information will be available when they need it
4. the systems they use will process information in a timely and trustworthy manner

In addition, information assurance extends to systems of all kinds, including large-scale distributed systems, control systems, and embedded systems, and it encompasses systems with hardware, software, and human components. The technologies of information assurance address system intrusions and compromises to information.

**What Can Happen**

It is remarkably easy to gain unauthorized access to information in an insecure networked environment, and it is hard to catch the intruders. Even if users have nothing stored on their computer that they consider important, that computer can be a “weak link,” allowing unauthorized access to the organization’s systems and information.

Seemingly innocuous information can expose a computer system to compromise. Information that intruders find useful includes which hardware and software are being used, system configuration, type of network connections, phone numbers, and access and authentication procedures. Security-related information can enable unauthorized individuals to access important files and programs, thus compromising the security of the system. Examples of important information are passwords, access control files and keys, personnel information, and encryption algorithms.

No one on the internet is immune. Those affected include banks and financial companies, insurance companies, brokerage houses, consultants, government contractors, government agencies, hospitals and medical laboratories, network service providers, utility companies, the textile business, universities, and wholesale and retail trades.

The consequences of a break-in cover a broad range of possibilities: a minor loss of time in recovering from the problem, a decrease in productivity, a significant loss of money or staff-hours, a devastating loss of credibility or market opportunity, a business no longer able to compete, legal liability, and the loss of life. Individuals may find that their credit card, medical, and other private information has been compromised. Identity theft can affect anyone.

Individuals who want to know more should read US-CERT Cyber Security Tips and other US-CERT papers. The US-CERT website contains papers, alerts, and other information for technical readers and for those responsible for government and control systems.