another way, *security depends on the appropriate protection mechanism of the weakest link in the entire security system*.

A company may have all the best cryptographic technologies installed in its computers and systems; however, all these protection efforts would collapse if someone (perhaps an intruder or an employee) can easily walk into offices and obtain valuable proprietary information that has been printed out as plaintext hard copy. Hence, one must not simply rely on cryptography-based security technologies to overcome other weaknesses and flaws in the security systems.

For example, if someone transmits valuable information as ciphertext over communications networks to protect confidentiality but stores the information as plaintext on the sender or receiver computer, it's still a vulnerable situation. Those computers must be protected to make sure the information is actually protected or kept confidential, possibly keeping the information in encrypted format as well—maybe with passwords to access the computer or folders or such. Also, the entire network must have strong firewalls and maintain those in secure facilities. The latter tasks are not of cryptography or cryptographic technologies. When building a secure system, we have to take into consideration a lot of issues of security, which are often dependent on the requirements and settings of the system.