Summary

Risk assessment is the cornerstone of risk management. When you are able to map all risk to the IT system and ultimately to the mission to a level of risk determination, the result leads to an understanding of how the potential exploitation of each risk will impact the organization's mission. If the *overall effects* of risks are determined to be high or critical, the necessary steps should be taken to mitigate such risk at the organization's earliest convenience. On the other hand, risks with overall effects rated as moderate to low can be deemed acceptable, requiring little or no response from management.

The discussion in this chapter, one could say, is purely academic. However, if the concepts are applied to real-world circumstances, the critical challenges in applying risk assessment techniques on a regular basis lie in two areas in the overall process. One critical challenge is developing a *realistic* estimate of the resources and capabilities that may be required to carry out an attack. Assessing the capability of a threat source is an extremely important stage in threat analysis. If the necessary due diligence is not devoted to attaining accurate information relative to attack capability, the effectiveness of the assessment is considerably compromised. The other critical challenge involves quantifying the impact of an exploited vulnerability. Again, if the quantification measurement that you use is not realistic, management may have a tough time accepting the recommendations of your risk assessment. Finally, once risks are determined, the appropriate steps should be taken against unacceptable risk.

For an excellent discussion on how to mitigate unacceptable risk and to conduct a cost-benefit analysis to justify acquisition of related security countermeasures, refer to the "Risk Management Guide," NIST Special Publication 800-30, which can be downloaded from the NIST (National Institute of Standards and Technology) Web site at www.NIST.gov.