In this short series of articles, I am updating materials I wrote for Chapter 28 (Security Policy Guidelines) of the *The Computer Security Handbook, 4th Edition*. This second column continues with recommendations on how to organize security policies.

Policies are distinct from the sequence in which they are presented. It is useful to have two distinct presentation sequences for policies: topical and organizational.

**Topical Organization**

Security involves a multitude of details; how one organizes these details depends on the purpose of the policy document. The most common format puts policies in a sequence that corresponds to some reasonable model of how people perceive security. For example, employees can look at security as a series of rings with a rough correspondence to the physical world. Under this model, one might have a policy document with a table of contents that looks like this:

- Principles
- Organizational Reporting Structure
- Physical Security
  - Servers
  - Workstations
  - Portable computers
- Hiring, Management, and Firing
- Data Protection
  - Classifying information
  - Data access controls
  - Encryption
  - Countering industrial espionage
- Communications Security
  - Perimeter controls
  - Web usage and content filtering
- E-mail usage and privacy
- Telephone and fax usage

- **Software**
  - Authorized products only
  - Proprietary (purchased) software
  - Development standards
  - Quality assurance and testing

- **Operating Systems**
  - Access controls
  - Logging

- **Technical Support**
  - Service-level agreements
  - Help desk functions

**Organizational**

The complete set of policies may be comprehensive, concise, and well written, but they will still likely be a daunting document, especially for nontechnical staff. To avoid distressing employees with huge tomes of incomprehensible materials, it makes sense to create special-purpose documents aimed at particular groups. For example, one could have guides like these:

- **General Guide for Protecting Corporate Information Assets**
- **Guide for Users of Portable Computers**
- **A Manager’s Guide to Security Policies**
- **Human Resources and Security**
- **Network Administration Security Policies**
- **Programmer’s Guide to Security and Quality Assurance**
- **The Operator’s Security Responsibilities**
- **Security and the Help Desk**

Each of these volumes or files can present just enough information to be useful and interesting to the readers without overwhelming them with detail. Each can make reference to the full policy document.