The Elements of Policy Style (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

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 first column starts with recommendations on how to frame security policies.

How should one write security policies? Should they be suggestions? Orders? Positive? Negative? I think that policies should be definite, unambiguous, and directive. In addition, all policies should have (preferably optional) explanations for the reasons behind them.

Orientation: Prescriptive and Proscriptive

Security policies should be written with clear indications that all employees are expected to conform to them. Language should be definite and unambiguous; e.g., “All employees must . . .” or “No employees shall . . .” Some policies require people to do something—these are _prescriptive_; e.g., “Employees must follow the password procedures defined by the Information Protection Group at all times.” Other policies prohibit certain actions—these are _proscriptive_; e.g., “No employee shall make or order illegal copies of proprietary software under any circumstances.”

Writing Style

Each policy should be short. Simple declarative sentences are best; writers should avoid long compound sentences with multiple clauses. Details of implementation are appropriate for standards and procedures, not for policies. Policies can refer users to the appropriate documents for implementation details; e.g., “Passwords shall be changed on a schedule defined in the _Security Procedures_ from the Information Protection Group.”

Reasons

Few people like to be ordered about with arbitrary rules. Trying to impose what appear to be senseless injunctions can generate a tide of rebellion among employees. It is far better to provide explanations of why policies make sense for the particular enterprise; however, such explanations can make the policies tedious to read for more experienced users. A solution is to provide optional explanations. One approach is to summarize policies in one part of the document and then to provide an extensive expansion of all the policies in a separate section or a separate document. Another approach is to use hypertext, as explained in an article to follow.

* * *

