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 fifth and final column provides suggestions on maintaining security policies.

There can be no fixed policy document that covers all eventualities. The information security field changes constantly, and so must policies. Information security is a process much like total quality management: for success, both require a thoroughgoing integration into corporate culture.

Above all, some named individuals must see maintaining security policies as an explicit part of their job descriptions. Hoping that someone will spontaneously maintain security policies is like hoping that someone will spontaneously maintain financial records. However, security policies should represent the best efforts of people from throughout the organization, not the arbitrary dictates of just one person.

**Review Process**

An information protection working group can meet regularly—quarterly is a good frequency to try—to review all or part of the policies. Employees can be encouraged to suggest improvements in policies or to propose new policies. The working group can identify key areas of greatest change and work on those first, leaving minor policy changes to subcommittees. Members of the working group should discuss ideas with their colleagues from throughout the enterprise, not just with each other. Every effort should contribute to increasing the legitimate sense of involvement in security policy by all employees, including managers and executives.

**Announcing Changes**

Drafts of the new versions can be circulated to the people principally affected by changes so that their responses can improve the new edition. Truly respectful enquiry will result in a greater sense of ownership of the policies by employees, although few of them will rejoice in the new policies. Some employees will see new security policies merely as a mild irritant, while others may view them as a tremendous obstacle to productivity, and a general nuisance.

Ideally, major changes in policy should be described and explained in several ways. For example, a letter or e-mail (digitally signed, one hopes) from the President, Chair of the Board of Directors, Chief Officers (CEO, CIO, CFO), or the Chief Information Security Officer can announce important changes in policy and the reasons for the changes. A brief article in the organization’s internal newsletter, or a spot on the intranet, can also provide channels for communicating the policy decisions to everyone involved.

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT.  Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>;  Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 M. E. Kabay.  All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.