I've been creating curriculum for the management module of Norwich University's Master of Science in Information Assurance (MSIA) program. Seminar Two of the six in the 18-month program consists of 11 weeks of study on foundation skills for IA managers, and Week Six is about management skills. In the module, one of the topics I put in is MBO -- Management by Objectives.

In a few words, MBO centers on the need and value of defining measurable objectives for a group. The theory is that unless we can measure performance and progress, our impressions of compliance with our goals will be too fuzzy and uncertain to motivate staff and to provide value to upper managers for strategic planning.

An important tool for MBO in the operations field is the service-level agreement (SLA). This agreement serves as a contract that defines acceptable service. For example, one can define the maximum acceptable rate of downtime for a network or the maximum acceptable response time for an application program. Knowing the limits is crucial for effective quality control; as staff see spikes or trends approaching the control limits, they can investigate the causes of irregular results or take action to correct appropriate factors before there’s a serious problem. Without stated limits, people may wait until there’s a disaster. When people rush around without a plan as they react to an emergency, everything is more expensive and more prone to error.

Applying MBO to information assurance, I'd say that it's not enough to use general terms like "be secure" or "protect information resources." I think that we should be using objectives such as "In the next three months, we will successfully prevent all unauthorized changes to our public Web server." We could use the concepts of SLAs to set a goal of ensuring a minimum available bandwidth for the network even in cases of denial-of-service attacks. Perhaps a good measurable objective might be “Find no more than 10% of all workstations logged on to the network after 8 pm every night.” How about, “Identify no more than 10% of all passwords by running crack programs on the password file?” Or “Limit porn-surfing on corporate machines to a maximum of 20% of total bandwidth during working hours?” If you do penetration tests, then it should be possible to define reasonable measurable objectives and then test those using the pen-tests.

Thinking in behavioral and measurable terms sharpens our ability to identify trouble spots and weak points in our security measures. Here’s a jingle you can set to music like the Burma Shave ads of the 1950s: “Sharpen up and apply MBO to IA today!”

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.

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.