One of the most troubling areas of information security is dealing with recalcitrant upper managers. I was sitting with a colleague in a class a while ago and heard a story that may send shivers up the back of any network security administrator.

My colleague -- let's call her Amy -- was the security manager at a major financial institution. She discovered that one of the managers from the accounting department had root access on the production systems for which she was responsible. Readers of this column will already know that no production systems should be accessible to anyone who does not need total control over that systems as part of their official responsibilities. Even within the production department, only a few people should ever have root access. In addition, one of the fundamental principles of security, whether for financial systems or for computers and networks, is the separation of duties. An accounting department manager with root access could easily initiate transactions and force them through production databases without supervision or detection.

Amy immediately went to talk to the accounting manager. Her normal strategy when dealing with anomalies was to assume that there must be a good reason for the situation and to investigate with an open mind. In contrast to some security managers I have known, Amy knew that adopting a hostile or authoritarian attitude would only cause resistance and resentment among her colleagues. Unfortunately, resistance and resentment where the immediate responses from the accounting manager. This man believed that having access to root was symbolic of his importance and power within the organization. He instantly took umbrage at Amy's questions and told her that he had no intention of giving up his root access or even of discussing the question further with her. Worse still, it turned out that this manager was the son of the CEO. He said that he would have Amy fired if she took away his root privilege.

If Amy succumbed to the threat, she would lose all credibility within the organization. If she challenged the abuse of power, she might get fired. Amy did the best thing she could under the circumstances: she removed the unwarranted root privileges at once and went directly to the CEO to discuss the situation. To her relief, the CEO supported her 100 percent. She never had any further conflict with the CEO's son; one can only imagine what the conversation was like between father and son.

This story illustrates an important principle: one must not confuse access with status. The CEO's son, for reasons unknown to the security manager, seemed to believe that his personal worth was bound up with his unnecessary access to system resources. Anytime this confusion occurs, it presents the potential for danger to the organization and conflict with fundamental principles of security.

I hope that this anecdote will help network managers reach their colleagues who still think that carrying the modern equivalent of a universal master key announces how valuable they are to the organization.
It's time to shred the illusions about worth, ego and access.

* * *

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 <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2001 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.