Walk What You Talk:
Upper Management Must Support INFOSEC

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

*The original version of this article was published in **Secure Computing Magazine** in 1995. The file is no longer available online, so we're republishing it here with minor updates.*

The VP of Finance was in a hurry. He did stop his headlong rush towards his office long enough to get a temporary security badge from the guard station, but then he just ran through the gate without using the card to trip the card reader. As he ran down the hall, the guard shrugged and reset the alarm. "Well," shrugged the guard, "at least he asked for a badge. Most of the senior executives here wouldn't even bother with that."

This incident occurred during my security audit of a large corporation in the early 1990s. One of the problems of the corporate culture at this client site was that most people did not wear their photo-ID cards visibly; they concealed them under jackets or sweaters. During meetings with top executives, it became clear why this should be: the top of the corporate ladder was setting a terrible example. Despite protestations of commitment to security, they showed contempt for security. The top echelons:

- Did not wear their badges;
- Insisted on one-letter passwords;
- Gave their secretaries their e-mail IDs and passwords instead of arranging for proxy rights;
- Demanded complete access to restricted zones such as the server room despite having no reason to be present alone in these areas.

It is much worse for security when high-ranking staff flout policies and procedures than when lower-ranking staff do. The problem is that people come to associate lack of respect for security with high rank – and so they imitate the behaviour consciously or unconsciously.

Consider the experience of e-mail implementers in the early years. One outstanding principle was enshrined in everyone's handbook of how to succeed at e-mail: start from the top and work down. If your boss used e-mail, you would too, simply to keep in contact. On the other hand, if only clerks used e-mail and senior executives disdained it, then middle managers and everyone else would avoid the new system because they unconsciously wanted to look important. The same phenomenon accounts in part for the resistance by some executives to direct keyboard interactions with their e-mail systems in the old days: they associated typing with secretaries and they looked down on secretaries despite their intense dependence on their colleague's competence and efficiency.

At one site I evaluated, a senior administrator insisted on having master keys that could open every single lock in the entire building, including dust closets. This person had confused access with power. In a similar vein, directors who demand access codes for secured areas where they have no business are sending a dangerous message to everyone else: ignore need to know – knowledge is power. How then are we security managers to counter the demand from the

programming manager to have access to the server room? And how will the programming manager deny access to production data to the programming staff? And then whither separation of duties?

The tendency to imitate high-status individuals is deeply rooted in our biology and in our culture. Among other primates, individuals cluster around alpha males and females as if the leader's power will leak over to them. In human societies, we see cults of personality worldwide. We find millions of people admiring and imitating screen and music stars. Children and adolescents, especially, wear special clothes to fit into their group; when was the last time you saw a teenager wearing a cap with the bill on the front? Adults spend inordinate time, money and effort buying new clothes simply to be "in fashion." So why would anyone think that these habits stop at the door to the workplace?

The workplace is a community – sometimes the only community we know. Like all communities, it has a culture: what many call the corporate culture. Within the corporate culture, there are leaders, either by virtue of their position in the hierarchy or by virtue of their personalities. If the leaders wear purple socks for a week, the frequency of purple socks among the rest of the staff will gradually increase. If the executives play golf, the middle managers will take up golf. This may strike some as silly, but it is inevitable. Human beings are social creatures. We can override our tendency to imitate but it is always part of us. It is because of these deep impulses, rooted in evolution and culture, that we have to convince upper management that they are crucial links in the chain of defence of corporate data. Without their example, the edifice of trust will crumble.

In America, the aboriginal peoples have a saying: Walk what you talk. It's time for upper management to walk what they talk.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *