Personnel Management and INFOSEC
Part 2. Ongoing Management: Opportunities for Abuse

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

In this series, we are reviewing some of the implications of personnel management for information security.

Security managers don't have to be paranoid, they just have to act as if they're paranoid. Work with your colleagues to help you identify behavior that indicates increased risk for your organization.

Treat people with scrupulously fair attention to written policies and procedures. Selective or capricious enforcement of procedures is harassment. If you allow some of your staff to be alone with the check run but force all others to be accompanied, the latter can justifiably interpret your inconsistency as an implicit indication of distrust. Such treatment may move certain employees to initiate grievances and civil lawsuits or to lay complaints under criminal statutes.

Inconsistency reduces your effectiveness. Suppose George is known for a no-nonsense, bluff manner. He sticks to technical issues with his staff; he rarely socializes with his colleagues and almost never talks about anyone's feelings. George discovers that his chief programmer, Sally, seems preoccupied and irritable lately. What is Sally to think when George suddenly enquires sweetly about how things are at home and whether she is under any strain? It would be easy for Sally to misinterpret George's apparent concern as either an unwarranted intrusion into her private life, a sexual come-on, or an accusation. George's unusual behavior could trigger alarm bells even in innocent employees.

In general, managers -- not just security officers -- should always be looking for opportunities to use the system in unauthorized ways -- no wait, wait, I mean so they can identify areas for improving security (you silly, twisted reader, you)!

What would you do if you discovered that an employee who used to occupy your current office still had the key? You would politely ask them to give it up. No one would question the reasonableness of such a request. However, when you remove access to the network server room from a system analyst who has no reason to enter that area, you may be treated to resentment, sulking and abuse. People learn about keys when they're children; they don't extend the principles to information security. People sometimes treat access controls as status symbols; why else would a CEO who has no technical training demand that his access code include the tape library and the wiring closet?

You can overcome these psychological barriers to better security by introducing a different way of looking at vulnerabilities. When you identify an opportunity to use the system in unauthorized ways, turn the discussion into a question of protecting the person against undue suspicion. For example, if one of your employees were found to have more access to secured files than required for her job, you could explain that having such capabilities put her at risk. If anything ever did go wrong with the secured files, she'd be a suspect. There's no need to frame the problem in terms of suspicion and distrust.
With these principles in mind, be alert to such opportunities as making an employee remain alone in a sensitive area, allowing unsupervised access to unencrypted backups, or having only one programmer who knows anything about the internals of the accounting package.

In the next piece in this series, I'll look at the problem of the indispensable employee.

* * *

M. E. Kabay, PhD, CISSP can be reached by e-mail at <mkabay@compuserve.com>.

AtomicTangerine is the Internet's first e-business venture consulting firm, combining the disciplines of venture capital, technology innovation and strategic consulting to create category killers and incubate new industries for companies of all sizes and at all stages of evolution. AtomicTangerine headquarters are in the San Francisco Bay Area and we have offices in New York, London, Tokyo, Washington DC, Boston, Denver and Seattle/Tacoma. Visit our new Web site at <www.atomictangerine.com>.

Copyright © 2000 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.