In this series, we are reviewing some of the implications of personnel management for information security. In this article, I examine the concepts of separation of duties.

The same principles that apply to the control of money should apply to control of data. Watch the tellers at a bank: when you deposit a large check, you'll see the teller going to a supervisor and having that person look the check over and initial the transaction. When bank tellers empty the automatic teller machines at night and fill the cash hoppers, there are always two people present. The person who creates a check is not the person who signs it.

In well-run information systems departments, data entry is distinct from validation and verification. For example, a data entry supervisor can check on the accuracy of data entry but cannot enter a new transaction without having their direct supervisor check their work. There is no excuse for allowing the supervisor to enter a transaction and then, effectively, authorize it. What if the entry were in error -- or fraudulent? Where would the control be?

In quality assurance for program development, the principles of separation of duty are well established. For example, the person who designs or codes a program must not be the only one to test the design or the code. Test systems are separate from production systems; programmers must not have access to confidential and critical data which are controlled by the production staff. Programmers must not enter the computer room if they have no authorized business there; operators must not modify production programs and batch jobs without authorization.

When I ran operations at a service bureau many years ago, I trained two systems managers as soon as I could to take over the day-to-day management of the computer systems. When they were ready, I asked them to remove system manager capabilities from my account. I had no wish to intrude on their province of responsibility. My meddling with system parameters would cause more trouble than it would solve. Were there to be an emergency, I could be granted system management permissions and resume my former role. This attitude exemplifies the concept of separation of duties.

In early 1995, the financial world was rocked by the collapse of the Barings PLC investment banking firm. The Singapore office chief, Nicholas Leeson, was accused of having played the futures market with disastrous consequences. The significant point in our context is that he managed to carry out all the orders without independent overview. Had there been effective separation of duties, the collapse would not have occurred.

A related approach is called dual control. As an example of dual control, consider the perennial problem of having secret passwords not know to management yet sometimes needing emergency access to those passwords. This problem does not generally apply to ordinary users' passwords, which can normally be reset by a security administrator without having to know the old password (and which are then changed to a truly secret string by the user after a single logon). However, if there is only one person who has the root password for a system (say, because the other system
manager is on vacation) then it makes sense to store a written copy of the root password in a truly opaque envelope, seal it, sign the seal, tape over the seal with non-removable tape, and then store the envelope in a corporate safe. The principle of dual control dictates that such a copy of the root password should be accessible only if two officers of the organization simultaneously sign for it when taking it out of the corporate safe.

In conclusion, think about the structure of control over information as you design your INFOSEC policies and make sure you are providing separation of duties or dual control throughout your systems.

***

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.