In this series, we are reviewing some of the implications of personnel management for information security. In two previous articles, I discussed some of the issues relating to the unreplaceable, indispensable employee and argued that such lack of shared knowledge is a security risk. In this article I examine why some people try to sequester knowledge and look at the issue of forced vacation time.

Sometimes a person continues to be indispensable because of fear that their value to their employer resides in their private knowledge. Such employees resent training others. The best way to change their counter-productive attitude is to walk what you talk: share knowledge with them and with everyone else in your group. Make education a normal part of the way you work. Encourage cross-training by allocating time for it. Make cross-training a factor in your employee evaluations. Have discussions of current topics from the trade press and academic journals. Start a journal club where people take it in turn to present the findings from recent research in areas of interest.

Reluctance to explain their job to someone else may also mask unauthorized or illegal activity. Take for example the case of Lloyd Benjamin Lewis, assistant operations officer at a large bank. He arranged with a confederate outside the bank to cash fraudulent check for up to $250,000 each on selected legitimate accounts at Lewis' branch. Using a secret code stolen from another branch, Lewis would scrupulously encode a credit for the exact amount of the theft, thus giving the illusion of correcting a transaction error. Lewis stole $21.3 million from his employer between September 1978 and January 1981, when he was caught by accident. For unknown reasons, a computer program flagged one of his fraudulent transactions so that another employee was notified of an irregularity. It did not take long to discover the fraud, and Lewis was convicted of embezzlement. He was sentenced to five years in a federal prison.

Since Lewis was obliged to be physically present to trap the fraudulent check as they came through the system, he could not afford to have anyone with him watching what he did. I doubt that Lewis would have been enthusiastic about having to train a backup to do his job. If anyone had been cross-trained, I doubt the embezzlement would have continued so long and been so serious.

Another even more sensitive topic is vacation time.

Lloyd Benjamin Lewis took his unauthorized duties (stealing money from his bank) so seriously that during the entire period of his embezzlement, about 850 days, he was never late, never absent, and never took a single vacation day in over two years. As a data center manager, I would have been quite alarmed at having an employee who had failed to be absent or late a single day in more than two years. How would you know what would happen if Mr Perfect really were away? The usual rule in companies is that if an employee fails to use vacation days, they can be carried over for a limited time and then they expire. This is supposed to be an incentive to take vacation time. For normal, honest employees it probably works fine. For dishonest employees who have to be present to control a scam, losing vacation days is irrelevant.
I recommend that every employee be required to take scheduled vacations within a definite -- and short -- time limit. No exceptions should be permitted. Excessive resistance to taking vacations should be investigated to find out why the employee insists on being at work all the time.

The problem is that the devoted, dedicated employee can get caught up in a web of suspicion precisely because of exceptional commitment. The only ways I can think of to avoid difficulties of this kind are (1) to make the reason for the policy well known to all employees so no one feels singled out; (2) to rely on the judgement and discretion and good will of the investigating manager to avoid hurt feelings in their most loyal employees.

* * *

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.