In this series, we are reviewing some of the implications of personnel management for information security. In a previous article, I discussed the approach to notifying an employee that (s)he has been fired. In this article, I want to look at what goes on behind the scenes to prepare for this difficult time.

Let's suppose the time has arrived for an employee and the employer to part company. In both resignations and firings, security consultants unanimously advise instant action. Not for them the leisurely grace period during which employees wind down their projects or hand them off to other staff members. No, security officers are a hard lot, and they advise the following scenario: in a formal exit interview, and in the presence of at least two managers, an officer of the employer informs the employee politely that his/her employment is at an end. During the exit interview, the officer explains the reasons for termination of employment. The officer gives the employee a check for the period of notification required by law or by contract (e.g., this could be at least the same period as that between pay checks) plus any severance pay due. Under supervision (preferably in the presence of at least one security guard), the employee is escorted to their work area and invited to remove all personal belongings and place them in a container provided by the employer. The employee returns all company badges, IDs, business cards available, credit cards, and keys. The employee is then ushered politely outside the building.

At the same time as all this is happening, all security arrangements must be changed to exclude the ex-employee from access to the building and to all information systems. Such restrictions can include:

- striking the person's name from all security-post lists of authorized access;
- explicitly informing guards that the ex-employee may not be allowed into the building, whether unaccompanied or accompanied by an employee, without special authorization by named authorities;
- changing the combinations, reprogramming access card systems, and replacing physical keys if necessary for all secure areas to which the individual used to have authorized access;
- removing or changing all personal access codes known to have been used by the ex-employee on all secured computer systems (microcomputers, networks, mainframes);
- informing all outside agencies (e.g., tape storage facilities, publications with company advertising) that the ex-employee is no longer authorized to access any of the employer's information or to initiate security or disaster recovery procedures;
- requesting cooperation from outside agencies in informing the employer if
ex-employees attempt to exercise unauthorized functions on behalf of their former employer.

The task is made more difficult by seniority or if the ex-employee played an important role in disaster recovery or security. The employer should be assiduous in searching out all possible avenues of entry resulting from the person's position of responsibility and familiarity with security procedures.

In one story circulating in the security literature, an employee was fired without the safeguards suggested above. He returned to the workplace the next Saturday with his station wagon and greeted the security guard with the usual friendliness and confidence. The guard, who had known him for years, was unaware that the man had been fired. The ex-employee still had access codes and copies of keys to secure areas. He entered the unattended computer room, destroyed all the files on the system, and then opened the tape vault. He engaged the guard's help in loading all the company's backup tapes into his station wagon. The thief even complained about how he had to work on weekends. This criminal then tried to extort money from the company by threatening to destroy the backup tapes, but he was found by police and arrested in time to prevent a disaster for his ex-employer.

* * *

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.