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

Crime is a human issue, not merely a technological one. True, technology can reduce the incidence of computer crimes, but the fundamental problem is that people can be tempted to take advantage of flaws in our information systems. The most spectacular biometric access control in the world won't stop someone from getting into your computer room if the janitor lets them in "just to pick up a listing."

Hiring new employees poses a particular problem; growing evidence suggests that many of us inflate our resumes with unfounded claims. Be especially careful of vague words such as "monitored," and "initiated"--find out what the candidate did in specific detail, if possible. Be sure that references are followed up at least to verify that the candidate really worked where the resume claims they did.

Unfortunately, there is a civil liberties problem when considering someone's criminal record. Once someone has suffered the legally-mandated punishment for a crime (fines, community service, imprisonment), discriminating against them in hiring may be a violation of their civil rights. Can you exclude convicted felons from any job openings? from job openings similar to areas in which they abused their former employers' trust? Are you permitted in law to require that prospective employees approve background checks? Can you legally require polygraph tests? Drug tests? You should consult your corporate legal staff to ensure that you know your rights and obligations in your specific legal context.

Even checking references from previous employers is fraught with uncertainty. Employers may hesitate to give bad references even for incompetent or unethical employees for fear of lawsuits if their comments become known or even if the employee fails to get a new job. Today, you can't even be sure you'll get an answer to the simple question, "Would you rehire this employee?"

Ex-employers must also be careful not to inflate their evaluation of an ex-employee. Sterling praise for a scoundrel could lead to a lawsuit from the disgruntled new employer.

For these reasons, a growing number of employers have corporate policies which forbid discussing a former employee's performance in any way, positive or negative. All you'll get from your contact in such cases is, "Your candidate did work as an Engineer Class 3 from 1991 to 1992. I am forbidden to provide any further information."

It is a commonplace in the security field that some people who have successfully carried out crimes have been rewarded by a "golden handshake" (a special payment in return for leaving) and even positive references. The criminals can then move on to victimize a new employer. For the same reasons that we cannot know exactly how many crimes are carried out, we can't tell how often this extortion takes place.
To work around such distortions, question the candidate closely about details their education and work experience. The answers can then be checked for internal consistency and compared with the candidate's written submissions. Liars hate details; it's so much harder to remember which lie to repeat to which person than it is to repeat the truth. Ask experienced employees to interview the candidate. Compare notes in meetings among your staff. I recall one new employee who claimed to have worked on particular platform for several years--but didn't know how to log on. Had he chatted with any of the programmers on staff before being hired, his deception would have been discovered quickly enough. Ironically, had he told the truth, he might have been hired anyway.

Before allowing new employees to start work, they should sign an employment agreement which stipulates that they will not disclose confidential information or trade secrets from their previous employer. Another clause must state that they understand that you are explicitly not requesting access to information misappropriated from their previous employer or stolen from any other source.

The Uniform Trade Secrets Act, which is enforced in many jurisdictions in the U.S., provides penalties which are triple the demonstrated financial damages caused by the data leakage plus attorney's fees.

* * *

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.