Payoff

The dynamic nature of the information systems and security professions creates an environment in which there is a high degree of turnover in employment. Turnover among systems and security specialists can expose the organization to damaging losses of information. This article addresses the risks involved and describes practices for hiring and terminating employees that can help minimize these risks.

Problems Addressed

In the past few years, the corporate world's image of the personnel function has undergone a significant change. An organization's employees are now considered a corporate resource and asset, requiring constant care and management. Changing legal conditions affecting personnel practices have underscored the need for clearly defined and well-publicized policies on a variety of issues.

The corporation and the employee have specific legal and ethical responsibilities to each other, both during and after the period of employment. Hiring and termination criteria, trade secrets, and noncompetition clauses are all issues that can cause serious legal problems for a corporation and its employees.

This article addresses personnel issues as they relate to information systems security, particularly hiring and termination procedures. Methods to protect both the corporation and the employee from unnecessary legal problems are discussed and problems regarding trade secrets and noncompetition clauses are reviewed.

The Professional Environment

The information systems and information security professions are in a vibrant and exciting industry that has always operated under a unique set of conditions. The industry relies on the unquestioned need for absolute confidentiality, security, and personal ethics. An organization and its reputation can be destroyed if its information security procedures are perceived as being inadequate or unsatisfactory. Yet, misuse or outright theft of software and confidential information can be relatively easy to accomplish, is profitable, and is often difficult to detect. Innovations can be easily transferred when an employee leaves the corporation, and information systems personnel have always been particularly mobile, moving between competitors on a regular basis.

These factors are extremely important as they relate to the corporation and its personnel practices. A newly hired programmer or security analyst, whose ethical outlook is largely unknown to management, may quickly have access to extremely sensitive and confidential information and trade secrets. Unauthorized release of this information could destroy the corporation's reputation or damage it financially. An employee who has just accepted a position with a major competitor may have access to trade secrets that are the foundation of the corporation's success.
Hiring Practices

Corporations must take special care during the interview to determine each candidate's level of personal and professional integrity. The sensitive nature and value of the equipment and data that employees will be handling require an in-depth screening process. At a minimum, this should include a series of comprehensive interviews that emphasize integrity as well as technical qualifications. References from former employers should be examined and verified.

The best way to verify information from an employment application is to conduct a thorough reference check with former supervisors, co-workers, teachers, and friends listed by the applicant on the application. Former employers are usually in the best position to rate the applicant accurately, providing a candid assessment of strengths and weaknesses, personal ethics, and past earnings, among other information.

Many employers have become increasingly cautious about releasing information or making objective statements that rate former personnel. Such employees have successfully sued corporations and supervisors for making derogatory statements to prospective employers. Many employers will furnish written information only about the applicant's dates of employment, positions held, and salaries earned, choosing to ignore more revealing questions. Often, an informal telephone check may reveal more information than would be obtained by a written request. If two large employers regularly hire each others' employees, it would be worthwhile for their personnel managers to develop a confidential personal relationship.

Use of a reference authorization and hold harmless agreement can help raise the comfort level of the former employer and get more complete information from a job applicant's previous employer. In such an agreement, the applicant authorizes the disclosure of past employment information and releases both the prospective employer and the previous employer from all claims and liabilities arising from the release of such information. An employer who uses such an agreement should require every job applicant to sign one as a condition of applying for employment. A copy of the agreement is then included with the request for references sent to the previous employer.

When sending or responding to a reference request that includes a reference authorization waiver and hold harmless agreement, it is important for employers to make sure that the form:

- Is signed by the job applicant.
- Releases the employer requesting the information as well as the previous employer from liability.
- Clearly specifies the type of information that may be divulged.

A responding employer should exercise extreme caution before releasing any written information about a former employee, even if the former employee has signed a reference authorization waiver. Only information specification permitted by the waiver should be released. If there is any ambiguity, the former employer should refuse to release the requested information. The former employer is safest if only the date of hire, job title, and date of termination are released.

Trade Secrets

A trade secret is a “formula, pattern, device, or compilation of information which is used in one's business, and which gives an opportunity to obtain an advantage over competitors who do not know or use it.” (Restatement of Torts, Section 757 (1939).) This advantage may be no more than a slight improvement over common trade practice, as long as the
process is not common knowledge in the trade. A process or method which is common knowledge within the trade is not considered a trade secret and will not be protected. For example, general knowledge of a new programming language or operating system that an employee may gain on the job is not considered a trade secret. The owner of a trade secret has exclusive rights to its use, may license another person to use the innovation, and may sue any person who misappropriates the trade secret.

Trade secret protection does not give rights that can be enforced against the public, but rather against only those individuals and organizations that have contractual or other special relations with the trade secret owner. Trade secret protection does not require registration with government agencies for its creation and enforcement; instead, protection exists from the time of the invention's creation and arises from the developer's natural desire to keep his or her invention confidential.

Strict legal guidelines to determine whether a specific secret qualifies for trade secret protection have not been established. To determine whether a specific aspect of a computer software or security system qualifies as a trade secret, the court will consider the following questions:

- Does the trade secret represent an investment of time or money by the organization which is claiming the trade secret?
- Does the trade secret have a specific value and usefulness to the owner?
- Has the owner taken specific efforts and security measures to ensure that the matter remains confidential?
- Could the trade secret have been independently discovered by a competitor?
- Did the alleged violator have access to the trade secret, either as a former employee or as one formerly involved in some way with the trade secret owner? Did the organization inform the alleged violator that a secrecy duty existed between them?
- Is the information available to the public by lawful means?

Trade secret suits are based primarily on state law, not federal law. If the owner is successful, the court may grant cash damages or injunctive relief, which would prevent the violator from using the trade secret.

**Trade Secrets and Personnel Practices**

Because information systems and security professionals often accept new positions with competitors, organizations seeking to develop and protect their information assets must take special care to determine each candidate's level of personal and professional integrity. The sensitive nature and value of the equipment and data that employees will be handling require an in-depth screening process. At a minimum, this should include a series of comprehensive pre-employment interviews that emphasize integrity as well as technical qualifications. Careful reference checking is essential.

When an employee joins the firm, the employment contract should expressly emphasize the employee's duty to keep certain types of information confidential both during and after the employee's tenure. The contract should be written in clear language to eliminate any possibility of misunderstanding. The employee must sign the agreement before the first day of work as a condition of employment and it should be permanently placed in his or her personnel file. A thorough briefing on security matters gives the employee initial notice that
a duty of secrecy exists, which may help establish legal liability against an employee who misuses proprietary information.

These secrecy requirements should be reinforced in writing on a regular basis. The organization should inform its employees that it relies on trade secret law to protect certain proprietary information resources and that the organization will enforce these rights. All employees should be aware of these conditions of employment.

The entrance interview provides the best opportunity to determine whether new employees have any existing obligations to protect the confidential information of their former employers. If such an obligation exists, a written record should be entered into the employee's personnel file, outlining the scope and nature of this obligation. In extreme cases and after consultation with legal counsel, it may become necessary to reassign the new employee to an area in which this knowledge will not violate trade secret law. Such actions reduce the risk that the former employer will bring an action for trade secret violation.

The employee should acknowledge in writing that he or she is aware of this obligation and will not disclose any trade secrets of the former employer in the new position. In addition, the employee should be asked if he or she has developed any innovations that may be owned by the former employer.

The organization should take special care when a new employee recently worked for a direct competitor. The new employer should clearly emphasize and the new employee should understand that the employee was hired for his or her skills and experience, not for any inside information about a competitor. The employee should never be expected or coerced into revealing such information as part of his or her job. Both parties should agree not to use any proprietary information gained from the employee's previous job.

**Trade Secrets and the Terminating Employee**

Even when an employee leaves the organization on excellent terms, certain precautions regarding terms of employment must be observed. The employee should be directed to return all documents, records, and other information in his or her possession concerning the organization's proprietary software, including any pertinent notes (except those items the employee has been authorized in writing to keep).

During the exit interview, the terms of the original employment agreement and trade secret law should be reviewed. The employee should then be given a copy of the agreement. If it is appropriate, the employer should write a courteous, nonaccusatory letter informing the new employer of the specific areas in which the employee has trade secret information. The letter should be sent with a copy of the employee's employment agreement. If the new employer has been notified of potential problems, it may be liable for damages resulting from the wrongful disclosure of trade secrets by the new employee.

**Noncompetition Clauses**

Many firms require new employees to sign a noncompetition clause. In such an agreement, the employee agrees not to compete with the employer by starting a business or by working for a competitor for a specific time after leaving the employer. In recent years, the courts have viewed such clauses with growing disfavor; the broad scope of such agreements severely limits the former employee's career options, and the former employer has no obligations in return.

Such agreements, by definition, constitute a restraint on free trade and are not favored by courts. To be upheld by the court, such agreements must be considered reasonable under the circumstances. Most courts analyze three major factors when making such determinations:
Whether the specific terms of the agreement are stricter than necessary to protect the employer's legitimate interests.

Whether the restraint is too harsh and oppressive for the employee.

Whether the restraint is harmful to the interests of the public.

If an employer chooses to require a noncompetition clause from its employees, care should be taken to ensure that the conditions are only as broad as are necessary to protect the employer's specific, realistic, limited interests. Clauses which prohibit an employee from working in the same specific application for a short time (one to three years) are usually not considered unreasonable. For example, a noncompetition clause which prohibits a former employee for working for a direct competitor for a period of two years may be upheld by the court, whereas a clause which prohibits a former employee from working in any facet of information processing or information security will probably not be upheld.

The employer should enforce the clause only if the former employee's actions represent a genuine threat to the employer. The court may reject broad restrictions completely, leaving the employer with no protection at all.

Precautionary Measures

Organizations can take several precautionary steps to safeguard their information assets. Perhaps the most important is to create a working atmosphere that promotes employee loyalty, high morale, and job satisfaction. Employees should be aware of the need for secrecy and of the ways inappropriate actions could affect the company's success.

Organizations should also ensure that their employee's submissions to technical and trade journals do not contain corporate secrets. Trade secrets lose their protected status once the information is available to the public. Potential submission to such journals should be cleared by technically-proficient senior managers before submission.

Intelligent restrictions on access to sensitive information should be adopted and enforced. Confidential information should be available only to employees who need it. Audit trails should record who accessed what information, at what times, and for how long. Sensitive documents should be marked confidential and stored in locked cabinets; they should be shredded or burned when it is time to discard them. (It should be noted that some courts have held that discarded documents no longer remain under the control of the creator and are in the public domain.) Confidential programs and computer-based information should be permanently erased or written over when it is time for their destruction. These measures reduce the chance of unauthorized access or unintentional disclosure.

Recommended Course of Action

To maintain information security, organizations should follow these steps in their personnel practices:

- Choose employees carefully. Personal integrity should be as important a factor in the hiring process as technical skills.

- Create an atmosphere in which the levels of employee loyalty, morale, and job satisfaction are high.
• Remind employees, on a regular basis, of their continuous responsibilities to protect the organization's information.

• Establish procedures for proper destruction and disposal of obsolete programs, reports, and data.

• Act defensively when an employee must be discharged, either for cause or as part of a cost reduction program. Such an employee should not be allowed access to the system and should be carefully watched until he or she leaves the premises. Any passwords used by the former employee should be immediately disabled.

• Do not be overly distrustful of departing employees. Most employees who resign on good terms from an organization do so for personal reasons, usually to accept a better position or to relocate. Such people do not wish to harm their former employer, but only to take advantage of a more suitable job situation. Although the organization should be prepared for any contingency, suspicion of former employees is usually unfounded.

• Protect trade secrets in an appropriate manner. Employees who learn new skills on the job may freely take those skills to another employer, as long as trade secrets are not revealed.

• Use noncompetition clauses only as a last resort. The courts may not enforce noncompetition clauses, especially if the employee is unable to find suitable employment as a result.

**Author Biographies**

Edward H. Freeman

Edward H. Freeman is an attorney and teacher in West Hartford, Connecticut. He has 19 years of experience in data processing and writes and lectures extensively on computer law and social issues, intellectual property and security.