Payoff
In addition to securing the data used and generated by computers, the organization must protect its software programs. The data security administrator must understand the legal measures available to ensure that software is adequately protected. This article presents an overview of the current laws regarding trade secrets, copyright, and patent law as they apply to computer software.

Problems Addressed
Organizations routinely invest in security systems to protect their data resources from unauthorized access, disclosure, destruction, or change. Similar security measures are necessary to protect an organization's software, whether written for outside sale or internal use only. Computer programs are a major corporate asset, and their design, development, and maintenance consume considerable corporate investment. Misuse or outright theft of software is easy to accomplish, profitable, and often difficult to detect.

This article discusses legal methods that organizations can use to protect their proprietary software. It includes a summary of the history, philosophy, and application of trade secret, copyright, and patent protection. Specific and practical steps that an organization can take to prevent or minimize potential problems are also discussed.

Trade Secret Protection
A trade secret is a formula, pattern, device, or compilation of information that is used in a business and that provides an opportunity to obtain an advantage over competitors who do not know the secret.\(^\text{27}\) 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. The owner of a trade secret has exclusive rights to its use, may choose to license another party to use the innovation, and may sue any person who misappropriates the trade secret.

There are several basic differences between the protection given by trade secret law and the protection given by copyright and patent. Trade secret protection affords rights that can be enforced not against the public but only against 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 innovation's creation and arises from the developer's natural desire to keep the work confidential. The owner of the trade secret must take reasonable and appropriate precautions to maintain the confidentiality of the innovation.

Strict 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 qualifies as a trade secret, the courts consider the following questions:

\begin{itemize}
  \item Does the information represent an investment of time or money by the organization claiming a trade secret?
  \item Does the trade secret have a specific value and usefulness to the owner?
\end{itemize}

\(^{27}\) Restatement of Torts, Section 757 (1939).
· Has the owner taken specific security measures to ensure that the information 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 someone formerly involved 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. The trade secret owner has the responsibility to prove its case in court. Depending on the likelihood of success and the level of potential damage to the trade secret owner, the court may grant a temporary restraining order, which would prevent the alleged violator from using the trade secret until the matter has been resolved. If the owner is successful, the court may grant cash damages, injunctive relief, and in some states, attorneys’ fees.

**Trade Secrets and Personnel Practices**

Because IS professionals often change jobs from one competitor to another, organizations seeking to develop and protect software 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.

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 so that there is no chance for any misunderstanding. The employee must sign the agreement before the first day of work as a condition of employment, and it should be retained as a permanent record in the employee's personnel file. A thorough briefing on security matters gives the employee initial notice that a secrecy duty 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 and that it will enforce these rights.

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 be necessary to reassign the new employee to an area in which this knowledge will not constitute a violation of trade secrets. Such actions minimize 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.
Trade Secrets and Terminating Employees

Certain precautions regarding terms of employment must be observed. The employee should be directed to return all documents, records, and other information concerning the organization’s proprietary software, including any pertinent notes (except those items for which the employee has written authorization to retain).

During the exit interview, the terms of the original employment agreement and trade secret law should be reviewed. The employee should be given a copy of the agreement. If it is appropriate, the employer should write a courteous, carefully worded letter notifying the new employer of the specific areas in which the employee possesses trade secret information. The letter should be sent with a copy of the employee's employment agreement. The new employer, if warned of potential problems, may be held 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—that is, 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 an agreement 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.

An employer that chooses to require a noncompetition clause from its employees should ensure that the conditions are only as broad as are necessary to protect the employer's specific, realistic, limited interests. Generally, clauses prohibiting an employee from working in the same application area for a short time (e.g., one to three years) are not considered unreasonable. The employer should attempt to enforce the clause only if the former employee's actions represent a genuine threat to the employer. The courts are particularly strict when the noncompetition clause interferes with the former employee's ability to make a living. They may reject broad restrictions completely, leaving the employer with no protection at all.

Precautionary Measures

Organizations can take several precautionary steps to safeguard proprietary software. 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.

In addition, organizations should ensure that their employees' submissions to technical and trade journals do not contain corporate secrets. Trade secrets lose their protected status once the information has been made available to the general public. Potential submissions to such journals should be cleared by technically proficient senior managers before they are submitted.
Commonsense restrictions on access to sensitive information should be adopted and enforced. Confidential information should be available only to employees who need it. Visitors should not be allowed in areas in which such information resides. Audit trails should show who had access to what information, at what times, and for how long. Documents should be marked confidential and stored in locked cabinets. Old printouts should be shredded or burned; some courts have held that such documents no longer remain under the control of the creator and are in the public domain. Confidential programs and data on disks and tapes should be permanently erased or written over. These measures reduce the possibility of unauthorized access or unintentional disclosure.

The organization must take special care when dealing with outside parties, particularly vendors, current and potential customers, and suppliers, who may become aware of trade secrets and other confidential information. The organization should require that third parties sign confidentiality agreements that protect the organization and limit the use of information being disclosed.

Copyright Protection

In Article I, Section 8, the US Constitution provides for copyright protection by empowering Congress to “promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.” Congress has regulated and upgraded copyright protection in a series of acts beginning in 1790. The courts have traditionally agreed that the words authors and writings are to be interpreted to mean more than printed materials because so many media(e.g., photographs and recordings) can be copyrighted.

Virtually every protection plan for proprietary computer software must address copyright. In some cases, copyright protection may be the only form of legal protection available.

Copyright protection is available for “original works of authorship fixed in any tangible medium of expression, now known or later developed for which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.” Since January 1, 1978, when the Copyright Revision Act of 1976 took effect, computer software and data bases have been defined as literary works by federal copyright laws. More specifically, literary works are defined as “works, other than audiovisual works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, periodicals manuscripts, phonograph records, films, tapes, disks, or cards in which they are embodied.” Thus, computer software and data bases are eligible for copyright protection when statutory requirements for copyright are present.

Basic Principles of Copyright

Copyright laws protect only the tangible expression of an idea. Ideas, concepts, principles, discoveries, procedures, processes, systems, and methods of operation in themselves do not qualify for copyright protection, although they may be protected as trade secrets or patents.

The sometimes unclear boundary between an idea and its expression has led to a great deal of copyright litigation. In many of these cases, especially when software is involved, the two items in the lawsuit may contain many similarities. In deciding whether copyright infringement has occurred, the courts frequently apply the test of whether the two works

---

28 Public Law 94-553 (October 19, 1976).
29 17 USC Sections 101, 102(a).
are substantially similar. Because copyright does not protect ideas, the court may consider that some similarities are unavoidable and perfectly permissible.

For example, if a company decided to create a new word processing package for sale to the office market, it would probably have many of the same features as older, copyrighted packages (e.g., functions for checking spelling, building indexes, and making pages). The developers might examine and study other packages to determine a method for creating these functions. Examining ideas and techniques used in other packages is not a violation of the copyright laws. If, however, the company also obtained a copy of the source code for another package and used it to create its own package, it would have copied the expression of an idea or ideas and its actions would be considered a violation of the copyright laws.

The Supreme Court illustrated the effect of this reasoning in an early case involving a copyrighted book that outlined a new bookkeeping system. The book detailed how the system worked and contained printed forms that could be used to implement the new system. Another author published a different set of forms, which accomplished the same purpose. The Supreme Court held that the first author’s copyright did not provide an exclusive right to make and use all bookkeeping forms based on the ideas expressed in the book, but only those forms that were actually a part of the book and copyrighted as such. The ideas of the bookkeeping system were not protected, only the actual forms used to implement the system. 30

**Rights of the Copyright Owner**

The owner of a copyright is granted several exclusive rights for the product, 31 which may be transferred by the owner to another party. Rights that might be useful for a software package include:

- The exclusive right to reproduce the package.

- The exclusive right to create derivative works based on the copyrighted work, including:
  - A translation of the package (e.g., from English to French).
  - An abridged version of the package, with some of its functions removed.
  - An upgraded or modified version of the original, containing new features.
  - A rewrite of the package in a different computer language or for a different computer.

- The exclusive right to distribute copies of the copyrighted work, through sale, rental license, or lease.

  In addition, the statutes specifically allow a legitimate user of a software package to make backup and archival copies. Those copies must be destroyed, however, when the “continued possession of the computer program [ceases] to be rightful.” 32

---

31 17 USC Section 106.
32 17 USC Section 117.
Translation of Copyrighted Software

Although it is clear to most that unauthorized line-for-line copying of a program infringes on the copyright, indirect copying or translation can present questions. In *Whelan v. Jaslow Dental Laboratories*, the Federal Court considered such a situation. In *Whelan*, the plaintiff designed and marketed a software package for the management of dental laboratories. The package was written in Event-Driven Language (EDL). After the sales representation agreement between Whelan and the defendant, Jaslow, was dissolved, Jaslow rewrote the software in Beginner's All-Purpose Symbolic Instruction Code and attempted to market the new version. The Beginner's All-Purpose Symbolic Instruction Code version duplicated the original system's functions, format, and screen layouts as well as its method of data storage, manipulation, and retrieval.

Jaslow admitted that Whelan's source code was used as a reference in writing the Beginner's All-Purpose Symbolic Instruction Code package. Jaslow also claimed that only Whelan's ideas, which were not copyrightable, were borrowed, not the expression of those ideas, which were covered under copyright law. Jaslow claimed that the end product was an expression of Whelan's ideas but was so dissimilar in appearance that it was a totally separate program and system.

The court rejected these arguments and held that copyright infringement had occurred, even though the two programs were written in different computer languages. The court said: The mere fact that the source code is written in Beginner’s All-Purpose Symbolic Instruction Code rather than EDL does not preclude the possibility of copying or copyright infringement. The idea of a computerized system to control a dental lab is not subject to copyright. The particular expression of that idea created and fixed in the plaintiff’s system is copyrightable, and the evidence demonstrates that the defendant did copy that expression in writing the source code.

Such cases as these leave the distinction between idea and expression unchanged. Jaslow did not simply use Whelan’s ideas in writing the Beginner’s All-Purpose Symbolic Instruction Code package but rather created a derivative work, more or less by simple translation. If a competitor wishes to write a package that functions similarly, other packages can still be researched and explored to evaluate the ideas, algorithms, and logic flow used. *Whelan* draws the line at wholesale derivatives of copyrighted software, especially when the new expression of the same ideas is secondary to mechanical translation techniques.

Similarity in Software Look and Feel

As software development and programming techniques have become more sophisticated, the approach used to create and write computer software has shifted. Several years ago, the emphasis was on the source code itself and the often tedious effort to ensure that the code actually did what the programmer intended. With the development of new interactive languages that facilitate source code development, software design and presentation—not program code—are becoming of primary importance. This design and presentation is referred to as the look and feel of the software.

The look and feel of software often contains more creative value than the actual source code. Software design is usually completed and approved before any code is written. Such factors as functions, features, screen design, command names, and data security are included in the specification and detail design phases of software development. This design phase can take longer and usually costs more than the actual programming effort. At a minimum, the design phase represents a tremendous amount of work and expense.

System designers want to protect this design effort against infringement by another party, even if no code has yet been written. Although it is clear that copyright law protects

---

the finished product, it is not clear that copyright extends to the protection of those elements constituting the product's design arrangement and execution.

A two-element standard for determining infringement was established by the US Court of Appeals for the Second Circuit in 1946. If substantial similarities do exist, it must be proved that the defendant had access to and copies of the plaintiff's copyrighted work and that the copying went so far as to constitute improper appropriation. The test for substantial similarity is whether the ordinary observer would recognize the copy as having been taken or appropriated from the copyrighted work.

This test, however, has been criticized when applied to software. The ordinary-observer test may be effective for music and plays, but the ordinary observer of software sees only screens and menus, which are just a small part of the design and development effort required to create a software package. A clever infringer could evade the copyright laws simply by designing the screens and menus while duplicating the internal logic flow.

Clearly then, the 1946 two-element standard for determining whether substantial similarity constitutes infringement does not answer the many new questions brought about by advances in software development methods and computer technology. A recent court decision deals with the problems created when two packages have the same look and feel but were written separately.

Lotus 1-2-3, which was developed by Lotus Development Corp., is the most popular computer spreadsheet package in the world. Paperback Software International developed its own package, which was much cheaper for customers to purchase. The Paperback Software package essentially mimicked the menus, commands, screen displays, structure, logic, and prompts of Lotus 1-2-3. Paperback had no access to the Lotus 1-2-3 source code.

In *Lotus Development Corp. v. Paperback Software International*, the court determined that certain aspects of the look and feel of a software package can be copyrighted. Such elements are copyrightable if the expression of the idea:

- Is the original work of the author.
- Is not so obvious that it is the same as the idea itself.
- Could have been expressed in several ways but was expressed in the same way as the original.

The court held that the idea of an electronic spreadsheet was not copyrightable, so anybody could design a package with the same features as Lotus 1-2-3. The concept of rows and columns on a spreadsheet could not be copyrighted, and the use of certain keys (e.g., arithmetic symbols, the enter key and the slash key) could not be protected.

The court then evaluated the remainder of the look and feel of Lotus 1-2-3, including such features as those keyboard functions, menus, screen displays, and command structures that are specific and unique to Lotus 1-2-3. In each case, the court determined that these features met the criterion required for copyright protection, and that Paperback Software had violated Lotus's copyright.

The *Lotus* test gives an organization an excellent indication of the level of protection that it can expect from the courts when a competitor creates a new package. The organization should be aware of the following points:

- The competitor may write a program that duplicates the capabilities of the original package.

---

34 *Arnstein v. Porter*, 154 F2d 464 (2d Cir. 1946).
The court will consider whether the competitor had actual access to the source code.

Certain accepted programming features (e.g., the use of certain accepted keys for specific functions) may be used without violating copyright law.

If there is substantial similarity between the look and feel of the two packages, the court will evaluate the original expression of the package's ideas in terms of originality, level of obviousness, and alternative methods of expression to determine whether a copyright violation has occurred.

In all cases, such matters should be handled by an attorney experienced in copyright litigation.

Copyright Registration

Copyright is probably the best protection for software. The copyright owner must take several steps, however, to avoid loss of the copyright itself or loss of certain remedies (e.g., the right to sue for infringement). All published, visually perceptible copies of the work must contain a notice of copyright consisting of three parts:

- The © symbol, the word copyright, or the abbreviation copr.
- The year of the work's first publication.
- The name of the copyright owner.

This notice should be displayed in several ways so it appears on all printouts of the program and on the user's terminal at sign-on. Notices should also be attached to labels on cartridges, diskettes, cassettes, and containers holding the copies of the program. If no copyright notice is given, copyright protection still applies, but a person who duplicates a program without notice may be held innocent of deliberate wrongdoing and therefore not liable for damages.

It is not necessary to register a copyright to establish its existence. Registration is required, however, to obtain the right to sue for copyright infringement and to collect damages. Because the actual registration procedure is complex, the organization should retain an attorney experienced in copyright to handle the process.

Work for Hire

Organizations often obtain the services of an outside contractor to write software packages. Such a contract is referred to as a work made for hire under Section 101 of the Copyright Act. These contracts, however, have raised the question of whether the organization or the outside contractor owns the copyright to the package, especially if the package is marketable outside the organization.

A 1989 Supreme Court decision, Community for Creative Non-Violence v. Reid, held that in some cases the outside contractor may retain certain copyright protection. In the absence of a written agreement, the courts make a decision based on the particular factors presented. Among the factors relevant to this inquiry are the skill required, the location of the work, the duration of the relationship between the parties, the extent of the contractor's discretion over when and how long to work, and the method of payment.

There is nothing in the Supreme Court's decision that precludes the employer from requiring that the contractor agree to assign all right, title, and interest in any copyrights it may develop during the course of the project. The employer and the outside contractor should work out a suitable agreement before any work is done. Such an agreement should clearly specify the rights and obligations of both parties in regard to the planned software package.

**Patent Protection**

Patent law has limited applications to computer software because few programs are likely to qualify for such protection. A patent may be obtained only for a “new and useful process, machine, manufacture, or composition of matter.” Current law, only computer software that is part of a patentable larger process or a part of machinery can be patented.

Patent protection is limited because of the time and expense involved in obtaining a patent, the limited scope of protection it affords once it has been obtained, and the difficulties likely to be encountered in enforcing a software patent. Because a patent provides the broadest form of protection, however, software developers should still consider such protection for software that is part of a larger process that would otherwise qualify for a patent. A patent obtains a monopoly over an invention for its developer for 17 years, during which time the patent holder can exclude others from making, using, or selling the patented invention.

**Recommended Course of Action**

To protect their investment, organizations that develop software, either for in-house use or external sale or lease, should:

- Choose employees and outside contractors carefully. Personal integrity should be as important a factor in the hiring process as computer skills.

- Create an atmosphere in which employee loyalty and morale, as well as job satisfaction, are high.

- Remind employees on a regular basis of their responsibility to protect the organization's proprietary information.

- Before any work is done by an outside contractor, put the rights and obligations of all parties into writing, particularly regarding ownership of the proprietary rights.

- Ensure that an attorney is involved in all copyright and contract processes.

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

Proprietary rights must be respected and treated in a manner consistent with their value to the organization. The organization should protect its software investment just as it protects its other assets.

**Author Biographies**

Edward H. Freeman

---

37 35 USC Section 101.
Edward H. Freeman is an attorney in West Hartford CT. He has 19 years of experience in data processing, most recently with a major insurance company. Freeman received an AA and a BA from Yeshiva University, an MS in computer science from New York University, and a JD from the University of Connecticut School of Law. He also holds a FLMI from the Life Office Management Association. In addition, he is a part-time faculty member at Central Connecticut State University and Gateway Community College, teaching computer and legal subjects.