Perhaps because of the low profile associated with trade secrets, they’re kept secret. Thus, there is no registration, trade secrets are protected only so long as they’re kept secret. Therefore, there is no registration process associated with trade secrets.

North Carolina recognizes trade secrets as business or technical information under the North Carolina Trade Secrets Act of 1990, a modified version of the Uniform Trade Secrets Act (UTSA), which has been adopted by a large majority of U.S. states. This recognition includes, but is not limited to, a formula, pattern, program, device, compilation of information, method, technique or process that:

1. Derives independent, actual, or potential commercial value from not being generally known or readily ascertainable through independent development or reverse engineering by persons who can obtain economic value from its disclosure or use; and
2. Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

A misappropriation occurs through the “acqui-

sition, disclosure, or use of a trade secret of another without express or implied authority or consent, unless such trade secret was arrived at by independent development, reverse engineering, or was obtained from another person with a right to disclose the trade secret.”

There is no single test for what “reasonable measures” are required to protect trade secret status, but common practices for businesses include:

• Identifying all trade secrets and, where practicable, labeling any such documents as “Confidential.”
• Informing employees about the sensitive nature of your trade secrets.
• Putting locks on doors of rooms and drawers or cabinets that contain sensitive material.
• Requiring visitors to sign in before entering a building where confidential material is housed.
• Requiring passwords for anyone accessing computers or networks.
• Providing employees with ID badges.
• Developing specific policies and procedures for hosting visitors (escorts, visitor badges, etc.).
• Having employees, contractors, and third parties of any kind with which you must share information during interviews, outside presentations, and any communication with others not subject to the protection of an NDA.

North Carolina lawyers and independent contractors with access to sensitive information should be reinforced through (1) dissemination of policy statements, memoranda and notices; (2) the use of sign-on screens on computers; (3) “Confidential” labels on sensitive materials; and (4) publication of a trade secret policy. The policy should be incorporated into the company employee handbook.

Businesses should also be careful with departing employees to ensure that trade secrets are maintained. Managers and/or human systems professionals should conduct exit interviews with the time the confidentiality agreement is signed, may be required in order to make the agreement enforceable. The confidentiality obligations of all employees and independent contractors who access to sensitive information should be reinforced through (1) dissemination of policy statements, memoranda and notices; (2) the use of sign-on screens on computers; (3) “Confidential” labels on sensitive materials; and (4) publication of a trade secret policy. The policy should be incorporated into the company employee handbook.

Continued on other side...
departing employees to obtain any materials and documents containing trade secrets still in the employee’s possession. This is also a good time to remind the employee of the obligations not to use or disclose the business’ trade secrets and/or confidential information even after termination of the employment.

Non-disclosure agreements are a particularly important tool in protecting trade secrets, but entrepreneurs would be wise to realize that not all NDAs are created equal, partly because there is not always an equal sharing of information by both parties. Frequently, vendors will share information about forthcoming products or future enhancements under an NDA, or a company contemplating a new project may issue a request for proposals under an NDA (to protect the sensitivity about the nature of the project). In either of those scenarios the information may be shared unilaterally.

The following is a partial checklist of considerations for reviewing an NDA, but business managers should generally seek legal help in reviewing or drafting one that is specifically tailored to their needs.

- The scope of the NDA is usually tied to a definition of Confidential Information (“CI”). Must CI be labeled as such to be considered confidential? How about information that is communicated verbally rather than in written form? Does the NDA attempt to reach back to include any information shared before the NDA was actually executed?
- Can the recipient share the CI with third parties under protection akin to the NDA signed with the discloser? Or, is the recipient prohibited from disclosing to all others at all times?
- How will court orders and subpoenas be handled? Must the recipient first alert the discloser that the CI has become subject to a court order and allow the discloser to file its own motions to limit the disclosure (e.g., by requesting that disclosure be kept under seal)?
- What treatment must the recipient give the CI upon termination or expiration of the NDA? Will all CI be returned? Or shall it be destroyed?

Trade secrets are protected only as long as they’re secret. Do not disclose or publically register information you want to keep secret. For example, a copyright defeats the purpose of a secret recipe.

Safeguard information and prevent misappropriation. Passwords, badges, and locks for doors and drawers keep secrets out of the hands of those who shouldn’t have them.

Make effective use of non-disclosure agreements (NDAs). Carefully tailor non-disclosure agreements to manage and control trade secrets among employees and vendors.