Protecting the Crown Jewels:

How to Prevent Trade Secret Misappropriation by Insiders

Christopher G. Smith

Susan H. Hargrove

Kayla J. Marshall

Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, LLP

150 Fayetteville Street, Suite 2300
Raleigh, NC 27601
(919) 821-1220
csmith@smithlaw.com

Christopher G. Smith is a partner at Smith Anderson. He leads the firm's business litigation team and is the Chair of the DRI Trade Secrets Practice Group. He has significant experience in business disputes, trade secrets, environmental litigation and risk management. He both prosecutes and defends claims, and advises clients on business risk management in a variety of areas.

Susan H. Hargrove is a partner at Smith Anderson. She focuses her practice on commercial litigation and dispute resolution with an emphasis in trade secret and non-compete matters.

Kayla J. Marshall is an associate at Smith Anderson, whose practice focuses on the areas of general litigation, commercial litigation, and employment litigation.

Protecting the Crown Jewels:
How to Prevent Trade Secret Misappropriation by Insiders

Table of Contents

Protecting the Crown Jewels:
How to Prevent Trade Secret Misappropriation by Insiders

I. Introduction

"Trade secrets" are generally defined as proprietary information that derives independent economic value from not being generally known or readily ascertainable by appropriate means by others. The scope of what constitutes a trade secret varies widely; trade secrets can include recipes (only seven people know how Thomas' English Muffins get their trademark "nooks and crannies"); step-by-step guides to create luxury (Starwood and Hilton have just settled after Starwood alleged that Hilton stole more than 100,000 trade secret files on developing their luxury brand hotels); and search algorithms (Google's proprietary search algorithm helped it establish dominance over the Internet).

Because of technological, business, and legal developments occurring in the last few decades, identifying and protecting trade secrets has become increasingly important for businesses. Currently, 48 states, and the District of Columbia, have enacted some version of the Uniform Trade Secrets Act ("UTSA"), and federal legislation has been introduced in Congress to federalize a cause of action for misappropriation. Despite these statutory measures, the misappropriation of trade secrets costs businesses billions of dollars. According to the Center for Responsible Enterprise and Trade, the annual economic impact of trade secret theft is one to three percent of the United States' Gross Domestic Product (GDP). Center for Responsible Enterprise and Trade, *Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats* (February 2014), available at http://www.pwc.com/en_US/us/forensic-services/publications/assets/economic-impact.pdf. Moreover, intangible assets have become increasingly valuable to businesses—in 2009, intangible assets of the 500 companies of the S&P 500 comprised 81 percent of the total value (compared to 17 percent of the companies' value in 1975). *See* James E. Malackowski, *The Intellectual Property Marketplace: Past, Present and Future*, 5 J. Marshall Rev. Intell. Prop. l. 605, 611 (2006). Trade secret litigation is booming—having doubled every decade over the past three decades, while federal litigation overall has decreased. Trade secret litigation in state courts has also increased over the past two decades at a faster rate than other types of state civil litigation. David S. Almelin *et al.*, *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 Gonz. L. Rev. 291, 301–02 (2010). Finally, dramatic changes in technology have had a significant impact on trade secrets. Digital storage of information makes it more difficult to protect trade secrets, compared to the days when trade secrets could be protected by simply locking a filing cabinet.

The increasing value of trade secret information, along with the ever increasing challenges in protecting that information, render trade secret protection more important than ever. Because misappropriation of trade secrets is often done by insiders, particularly employees, it is crucial that companies invest time identifying trade secret information and taking reasonable steps to safeguard their confidentiality at each stage in the employment process—before the employment relationship begins, during the employment relationship, and after the employment has ended. It is also important that companies be prepared to respond to and initiate litigation protecting trade secrets. These steps will help companies prevent the misappropriation of trade secrets by insiders in the first instance, and maximize the opportunity to enforce a company's trade secret rights in the event of an emergency or other dispute.

II. Before the Employment Relationship Begins

A. Identify Your "Crown Jewels"

In order for information to receive trade secret protection under the UTSA, (1) the information must derive independent economic or commercial value from not being generally known or readily ascertainable by appropriate means by others; and (2) the information must be the subject of reasonable efforts to maintain its secrecy.

Assessing what information is protectable under the UTSA is an important first step in identifying the "crown jewels" of the company. For information to receive trade secret protection, the information cannot be generally known or readily ascertainable by a person or entity acting properly and within the law. Information might be generally known or readily accessible if an outsider could compile the information on his or her own. For example, in *Novacare Orthotics & Prosthetics E., Inc. v. Speelman*, 137 N.C. App. 471, 478, 528 S.E.2d 918, 922 (2000), the court held that customer lists were not trade secrets because the information used to contact the clients would have been readily accessible through a local telephone book. Similarly, in *Carbonic Fire Extinguishers, Inc. v. Heath*, 190 Ill.App.3d 948, 952–53, 138 Ill.Dec. 508, 547 N.E.2d 675, 677 (1989), the court held that the customer list and pricing information of a business that cleaned restaurant hoods was not a trade secret because "although the actual customers using plaintiff's services are not readily apparent from the telephone directory, anyone seeking to compete with plaintiff, including defendant, could very likely encounter plaintiff's customers by simply contacting restaurants through the telephone directory."

Related to the question of whether information can be readily ascertainable is whether information has independent actual or potential commercial value. It is logical that information that could be readily ascertained by proper means would be unlikely to have independent commercial value. To demonstrate that the information has commercial value, courts may look to whether the information gives the company a competitive edge over others; whether marketing would pay for the information, and the amount of effort or money expended in developing the information. Taking publicly available information and doing something special with it can elevate the status of that information and make it a trade secret. For example, in *Amoco Production Co. v. Laird*, 622 N.E.2d 912, 917–18 (Ind.1993), the court held that information regarding the location of potential oil fields was a trade secret because highly skilled employees, using some information in the public domain, invested seven months in exploratory work, and the company spent $150,000 to have an outside contractor conduct an airborne microwave radar survey of a 13,000 square mile area. See also *Byrd's Lawn & Landscaping, Inc. v. Smith*, 142 N.C. App. 371, 375–76, 542 S.E.2d 689, 692 (2001), in which the court held that the evidence was sufficient to support a verdict where the customer list included cost history of bidding information with respect to each customer. The plaintiff had used that information to prepare bids, and he taught the defendant how to prepare bids using that information. The defendant started his own business and underbid the plaintiff on eleven of fourteen properties on which the plaintiff had previously had the contract. Compare to *Carbonic Fire Extinguishers, Inc. v. Heath*, 190 Ill. App. 3d 948, 953, 547 N.E.2d 675, 677 (1989), in which the court concluded that a restaurant hood cleaning business's list of customers was not economically valuable because its development "would entail little, if any, expense beyond that ordinarily required to establish a customer relationship." Similarly, in *Applied Indus. Materials Corp. v. Brantjes*, 891 F. Supp. 432, 439 (N.D. Ill. 1994), the court determined that the net profit derived from the purchase and sale of petroleum coke was not a trade secret because the information was so outdated that it lacked current economic value.

Some of these results may seem inconsistent, but in each instance the Court is assessing the *independent value* of the information at issue. In *Byrd's Lawn*, it was evident that the information was very valuable

given the success that the bad actor had making unauthorized use of it. In *Carbonic Fire Extinguishers* and *Applied Indus.*, no such value was demonstrated and thus the results were different.

Moreover, courts have stated that to plead misappropriation of trade secrets, a plaintiff "must identify a trade secret with sufficient particularity so as to enable a defendant to delineate that which he is accused of misappropriating and a court to determine whether misappropriation has or is threatened to occur." *Vision-AIR, Inc. v. James*, 167 N.C. App. 504, 510–11 (2004). A complaint that makes general allegations in sweeping and conclusory statements, without specifically identifying the trade secrets allegedly misappropriated, is insufficient to state a claim for misappropriation of trade secrets and therefore, is subject to dismissal under Rule 12(b)(6). *Washburn v. Yadkin Valley Bank & Trust Co.*, 190 N.C.App. 315, 327 (2008). In *Washburn*, the court held that the defendant had not identified with "sufficient specificity" either the trade secret that the plaintiffs allegedly misappropriated or the acts by which the alleged misappropriation were accomplished. The court stated that the identification of the trade secrets was "broad and vague" where the defendant claimed that the plaintiffs acquired business methods, clients, their specific requirements and needs, and other confidential information pertaining to the defendant's business. Similarly, in *Panos v. Timco Engine Ctr., Inc.*, 197 N.C. App. 510, 519, 677 S.E.2d 868, 875 (2009), the court held that the defendants did not state a claim for misappropriation where the defendant was unable to identify the trade secret information that the plaintiff allegedly improperly used because the plaintiff had deleted all of the information stored on his company-issued computer. The court rejected the defendant's argument that the plaintiff's alleged spoliation of evidence justified an inference that the information erased from plaintiff's hard drive constituted trade secrets and that the plaintiff misappropriated that information.

These cases all can be grouped around the concept of proof of *independent value*. Information should not receive special trade secret protection if you cannot show its value. In *Panos* above, the plaintiff could not even show what the information was, accordingly nor could it show actual value. *Panos* is a nice segue way into a core concept of protecting special information, *i.e.*, building a culture of respect for confidential information.

B. Build a Culture of Respect for Confidential Information

When it comes to protecting the crown jewels of your business, there is no substitute for developing and maintaining a top down corporate culture that expects and demands respect for maintaining the confidentiality of the corporation's information. Developing such a culture is essential to demonstrating the independent value of the client's information. Your clients will be making significant strides in that direction if they will follow the three "C"s of the Culture of Confidentiality:

- Clarify: Identify the information that is important to protect. The corporate admonitions to safeguard information will be taken more seriously if they are applied judiciously to genuinely confidential information.
- Communicate: Share the company's expectations regarding what information is confidential and how that confidentiality needs to be protected early and often. These expectations should be discussed during intake at the inception of employment and re-enforced with appropriate confidentiality clauses and handbook provisions. They should be sustained by appropriate classification and marking of confidential information and continuing training regarding the scope of confidential information and its importance to the company. They should be reiterated at the exit interview when all company information, data and devices are collected and the company's expectations about the integrity of the employee's post-separation behavior are discussed.
- Commit: The caretaking of confidential and trade secret information is not a "one size fits all" nor is it a checklist item that can be completed and forgotten. The nature of confidential and

trade secret information is dynamic and assuring its protection requires a commitment to focusing on its importance over time and at all levels.

C. Build the Fortress: Put in Place Safeguards Necessary to Protect Your Crucial Information

Using safeguards to protect crucial information is important for two reasons: first, it will help prevent the misappropriation of trade secrets by making it more difficult for employees to steal the information, and second, information will not receive trade secret protection unless the company has demonstrated that it has used reasonable means to protect the information. Courts have not identified any particular measures that alone are necessary or sufficient to demonstrate that companies have taken reasonable measures; instead, courts evaluate the measures on a case-by-case basis to determine if they are reasonable under the circumstances. Many of the measures considered by courts in determining whether an employer's efforts were reasonable have been whether companies keep information under lock and key; limit computer or building access; denote documents as confidential, or require confidentiality or non-compete agreements. *See e.g. Strata Mktg., Inc. v. Murphy*, 317 Ill. App. 3d 1054, 1069, 740 N.E.2d 1166, 1177 (2000); *Starsurgical Inc. v. Aperta*, LLC, No. 10-CV-01156, 2014 WL 4072117 (E.D. Wis. Aug. 14, 2014).

1. Limit Access to Information

Once you have determined the universe of your trade secret information, you will be in a position to identify the employees in your company who need to have access to that information in order to do their jobs, and can limit access to those individuals. One way to do this is by compartmentalizing data and limiting access by geographic region or job function, and by using passwords to prevent unauthorized access. For example, customer information should be available only to those who need it, but not freely accessible to those without active business relationships with those customers.

Although most information is stored electronically, it is important to limit access to information in its tangible form as well. Limit the number of copies of confidential documents and, for especially sensitive information, use control numbers with records kept as to authorized recipients.

2. Implement Technology Policies

Certain technical safeguards should be implemented to protect trade secret information. Some recommended steps to safeguard information, depending upon the circumstances, can include:

- Mark all genuinely confidential documents as such.
- Encryption where appropriate of critical information to prevent it from being emailed, downloaded, copied, or printed.
- Establish firewalls to isolate confidential from non-confidential information on the server.
- Use security software that prevents outgoing emails from attaching sensitive company information. (The software scans for key words and sequesters any documents containing those words until reviewed internally.)
- Remote work should be done on company-owned computer or through a direct connection to the employer network. Allowing employees to work remotely from personal devices leads to retrieval problems and may suggest insufficient safeguards were taken to protect the information.
- Where appropriate, consider disabling USB ports on company computers to avoid the capacity to download sensitive information to a portable device.

- Develop a policy on employees' use of their own devices for work purposes as well as use of cloud storage. Consider prohibiting use of personal Dropbox and other cloud storage services.

3. Develop a Strong Partnership with the IT Department

Once management has determined the universe of documents that require protection, it is essential to collaborate with the company's information technology department as well as its human resources personnel to determine what security measures are appropriate, feasible and cost effective, and to ensure that the policies implemented are clearly communicated and consistently followed.

At the same time, the professional obligation to be able to secure your client's information is accompanied by the professional obligation to be conversant in technology issues as a practitioner. Comment 8 of Rule 1.1 of the American Bar Association Model Rules of Professional Conduct provides that "a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology" in order to maintain competence. As noted throughout this manuscript, technology, understanding it and using it properly, is an essential part of the foundation of the fortress to protect the company's crown jewels. Counsel cannot properly manage risk and help architect those steps without adequate practical proficiency.

By putting into place these measures before the employment relationship has even begun ensures that once an individual is hired, the trade secret information has already been identified, and measures have already been implemented to ensure its protection.

III. During the Employment Relationship

Once the employee is hired, it is necessary to set clear expectations with employees that the company's proprietary information is confidential. Confidentiality agreements, and non-competes are important tools for companies to use to identify which information is confidential and to establish how the confidential information can be used or disclosed.

Confidentiality Agreement. This should be tendered to the employee at the time of employment and made a condition of the offer, and signed on or before the first day of employment and again at termination. Although a confidentiality agreement may not be sufficient alone to fulfill UTSA's requirement that companies take reasonable measures to protect confidential information, it is an important factor that courts will consider. *Compare Arcor, Inc. v. Haas*, 363 Ill. App. 3d 396, 842 N.E.2d 265 (2005) (holding that the employer did not take reasonable steps to keep its customer information secret where the only security measure employer took was to have its employees sign an employment and confidentiality agreement); and *UTStarcom, Inc. v. Starent Networks, Corp.*, 675 F. Supp. 2d 854, 866-67 (N.D. Ill. 2009*)* (holding that where the customer list was developed slowly and through hard work, stored in a secure location, and shared with employees on a need-to-know basis and only after they signed confidentiality agreements, the list may qualify as a trade secret).

In the confidentiality agreement, identify the company's confidential information and establish permitted uses and disclosures of the confidential information. The policy (and the confidentiality agreement) should have consistent terms and, among other things, include the following commonly omitted terms: (1) address use of external storage devices; (2) ban use of personal storage devices (for example thumb drives) and email of company documents to personal email accounts; (3) prohibit installation of unapproved software; (4) prohibit cleaning, defragmentation of employee computer by the employee; and (5) if employees are permitted to use personal devices (mobile phones, tablets, computers) for work purposes, require deletion of all information that may reside on the those devices at the time of termination of employment, preferably by the company's IT department.

It's not enough to institute a confidentiality policy. To demonstrate commitment to the protection of confidential information, that policy must be enforced or else it will not assist in establishment of a trade secret. (*See, e.g. Merck & Co. v. Lyon,* 941 F. Supp. 1443 (M.D.N.C. 1996), noting that a company had failed to follow its own policy of a tiered designation of documents as "critical", "restricted" and "confidential" when it imposed a "restricted" designation on documents that were not confidential.) It is also useful to conduct ongoing employee awareness and training programs about confidentiality of company information.

Non-Compete. Have the employee sign a non-compete where appropriate. A well-crafted non-compete is not only a useful tool to inhibit misuse of trade secret information, it serves as an indicator of the company's efforts to protect its information. There are significant variations among states regarding the enforceability of non-competes, so it is necessary to research statutes and case law to appropriately tailor the non-compete for the employee.

Continuous assessment. Assessing the universe of your trade secrets must be an ongoing process. Companies accrue new trade secret information over time, existing information may gain or lose trade secret status, and technological advances will almost certainly alter what protections are available and reasonable. Thus, a procedure that requires a periodic audit of the universe of trade secret information and the procedures implemented to protect it is essential.

IV. After the Employment Relationship Has Ended

Once the employment relationship has ended, it is important to act quickly to ensure that the departing employee does not take with him or her important confidential information.

A. Terminate Access Immediately

As soon as the employee's employment with the company has ended, terminate the employee's access to the physical premises, systems, computers, hard drives, memory devices, email and phones.

- Physical premises:
  - obtain security access cards
  - change access and security codes when appropriate
- Systems:
  - remove network rights
  - disable remote access to network
  - change passwords for all applications to which employee had access via the server
  - remove administrator rights, if any
- Computer:
  - obtain custody of desktop and/or lap top computer and any tablets
  - disable Windows log-in account
  - change passwords for all applications on computer
  - remove employee's personal files from system/computer, including any personal email folder
- Hard drives and memory devices:
  - obtain custody of all company external hard drives and memory sticks
- *if there is any anticipation of a potential dispute or risk management issue, have a forensic image prepared of all devices*

- Email:
  - disable email account
  - disable remote email access
- Phones:
  - obtain custody of cell phone
  - delete voicemail account or change the password
  - update phone directory (hard and electronic)
- Files:
  - take inventory of all files/projects on which individual was working; ensure that all materials are returned (very important if employee worked remotely)
- If the employee used non-company devices, take steps to ensure that all company data has been removed from those devices.

B. Conduct Timely Assessment of Electronic Devices

Ensure company information is not being downloaded or sent to personal email accounts. In involuntary terminations or other departures that might raise a "yellow" flag, the company may consider conducting a pre-notification examination so as to be able to determine whether suspicious activity occurred after the notification.

C. Conduct an Exit Interview

The exit interview provides an important opportunity to ensure that the company has secured all information that was available to the employee, to remind the employee of all post-termination obligations regarding confidential information and non-competition, and to gain intelligence about the employee's future plans. At the exit interview of any employee who has had access to sensitive information, at least one supervisor or management representative knowledgeable about the nature and scope of the employee's assignments should be present. In the exit interview:

- Review and audit the departing employee's paper and electronic documents.
- Question the employee about information that may remain in his or her possession.
- Review any confidentiality agreements or non-competes.
- Question the employee about his or her future plans.
- Where appropriate, send copies of confidentiality and non-compete agreements to the new employer of your departing employee.

There is lots of room for good business judgment in these situations. Depending on the size of a company, it probably is not practical in each departure to perform a pre-interview forensic examination of the employee's electronic devices, which might show evidence of deletions, downloading, cleaning or defragmentation. But companies should have in mind that in the proper situation, where the departing employee had access to the crown jewels, these additional steps should be considered as part of the exit process.

The exit interview is also a good opportunity to question the employee about his or her next employment, including the specific job duties and nature of the her work. If the employee's next employment is with a competitor, that may be a red flag to the employer to ensure its trade secret information has been adequately protected. In some jurisdictions, a court may intervene to prohibit subsequent employment by a competitor of an employee possessed of particularly important trade secret information even in the absence of a noncom-

pete agreement. *See PepsiCo, Inc. v. Redmond*, 54 F.3d 1262 (7th Cir. 1995). In addition to being the seminal case on the inevitable disclosure doctrine, in *PepsiCo*, the court took a dim view of the departing employees' evasive responses to questions at his exit interview about his future employment intentions. This case and others like it highlight the potential value to the client of the exit interview process. Evasive answers during that process by an employee who then goes to a competitor naturally raise suspicion and courts properly grow concerned at lack of candor. *See also TSG Finishing, LLC v. Bollinger*, No. COA14-623, 2014 WL 7463824 (N.C. Ct. App. Dec. 31, 2014) (holding that an employer made a prima facie showing of former employee's misappropriation of its trade secrets, as a basis for obtaining a preliminary injunction, where the former employee went to work for employer's competitor; employee was asked to perform similar duties for competitor that he had performed for employer; employer and competitor shared customers; employee was working for some of same customers that he had worked for with employer for whom he had developed specialized processes for; and employee admitted that he talked about various components of employer's specialized data cards for each process with competitor's management personnel).

Finally, document the exit interview, including the employee's acknowledgement of his or her duties to the company and the return of company property and information provided about next employment (including specific job duties and nature of projects). Send a follow-up letter to the individual detailing the exit interview acknowledgements and continuing obligations.

D. Be Aware of Warning Signs

Pay attention to possible warning signs of potential theft, including if the employee refuses to disclose the identity of a new employer or new assignments; works unusual hours in final days (early, late, weekends); or gives little or no notice of resignation. If these warning signs are present, consider a forensic examination of the former employee's hard drive to determine if theft has occurred.

V. The Dispute

Even with a strong fortress and a culture of respect, trade secret theft may still occur. By instituting the foregoing measures, businesses will maximize the opportunity to enforce their trade secret rights if an emergency arises. It is important to be prepared in order to act quickly and deliberately if trade secret theft is suspected. Here is a broad outline of the process steps to follow when concern arises and the client may need to take enforcement action.

A. Investigate When Warning Signs Are First Detected

- Have a forensic copy made of all of employee's devices.
- Identify the universe of information to which the departing employee had access, especially at time of departure.
- Identify the subset of the information to which the employee had access that has commercial value by virtue of not being widely known or readily ascertainable.
- Identify mechanisms in place to protect the trade secret info to which employee had access.
- Determine the utility of the employee's information pipeline to his or her new employment situation, which you will have learned during the exit interview.
- Consider interviews of persons who worked closely with the employee to determine whether employee disclosed plans, intents or activities that would be relevant to his future actions and his use of information.

- Perform a review of the employee's devices to check for evidence of improper transfer (USB drives plugged into a device at a time close to departure for suspiciously extended periods of time, opening of sensitive documents at the same time the USB drive was connected to the employee device; sending documents to personal email addresses as email attachments).
- Assess available claims:
    - Are you protected by a non-compete agreement with the employee?
    - Do you have a confidentiality agreement with the employee that clearly identifies the information to which it pertains?
    - Are you in a jurisdiction in which the Computer Fraud and Abuse Act recognizes access with intent to misuse as unauthorized and therefore triggering the statute?
    - Did employee have access to trade secrets (this will turn on analysis of the information gathered in response to the audit bullet points outlined above in bullets 2-4).

B. Determine Next Steps

After investigating the possible trade secret misappropriation, it is necessary to decide what steps to take next, including whether to sue or settle the dispute out of court, and if pursuing litigation, whether to demand an injunction or damages. This ultimately is a business judgment which will turn on assessment of the following factors:

- How hot is the information? The more helpful the data would be to a competitor, the more aggressive you will want to be about making sure you keep it out of their hands, as opposed to trying to get them to pay you for it later.
- How solid is your evidence of misappropriation? If your forensics clearly lead to a reasonable conclusion that important stuff was taken such that additional discovery is not needed to make a misappropriation argument, you can be more confident in pursuing emergent injunctive relief.
- How able are you to identify your trade secret information with particularity? Seeking to prevent an employee from using a confidential pricing algorithm or a specific research protocol being used to test a product under development will be more likely to be successful than asking that a court keep a former employee from using your marketing information, business plans or operational processes.
- There is a risk to delay. To obtain an injunction you need to convince a judge that the relief you are requesting is necessary to prevent irreparable harm from being visited upon your client. A delay in proceeding to seek an injunction can be used by your adversary as evidencing a lack of urgency. But,
- The pursuit of a preliminary injunction is pricey. You need to demonstrate a likelihood of success on the merits, which commands marshaling affidavit evidence as well as compelling legal arguments. It is somewhat like trying to take the work done over a year or two to prepare for a trial and compressing it into a six or seven week period.
- Consider your intelligence about the employee or his subsequent employer, if there is one. Will they be likely to cooperate with an overture to resolve the matter in ways that protect your information?
- Consider the result that you would like to see to protect the company and determine whether that is available to you and what the best path to obtain it would be. Is return of the USB with an

affidavit that there are no copies sufficient? Is the information so crucial and so ingrained in the brain pathways of the departing employee that nothing short of keeping him out of the field until the information becomes outmoded will suffice?

VI. Conclusion: Ten Suggestions for Trade Secret Protection

Protecting a business's trade secrets is an ongoing process, which includes identifying protectable and important information; developing a culture of confidentiality; building a fortress around the trade secrets; and taking swift action to secure information when employees depart. The following ten steps are key to this process.

1. Understand the nature and scope of the information you are trying to protect.
2. Secure the information in a manner that is appropriate to its value and significance.
3. Don't neglect electronic safeguards, passwords, limited access, and emphasize need to know when making access decisions.
4. Obtain non-compete and confidentiality agreements appropriate to the information you are trying to protect.
5. Consider security implications of work at home or Bring Your Own Device policies.
6. Consider carefully the security protective in any off-site storage systems.
7. Have new hires acknowledge in writing your expectation that they will not use confidential information of others.
8. Use nondisclosure agreements with customers and vendors where appropriate.
9. Conduct a comprehensive exit interview, collect all company electronic devices.
10. If you expect misappropriation by a departing employee, have a forensic image made of all electronic devices.