Texas Business Guide: Identifying and Protecting Trade Secrets
Under the (New) Texas Uniform Trade Secrets Act

Shawn E. Tuma
shawn.tuma@solidcounsel.com
www.solidcounsel.com
214.472.2135
Why Use This Guide?

Virtually every business has trade secrets, that is, something unique or remarkable about the way it makes a product or provides a service that sets it apart from the competition. This is something that gives it a competitive advantage and is usually something it has spent significant time and resources to develop.

Unfortunately, in today’s business environment, honor and integrity are not always the rule and many businesses find their trade secrets are being taken and used to compete against them. This can come from as close as disloyal employees or local competitors to around the world from foreign state-sponsored businesses engaging in industrial espionage.

Preparation is the Key to Success

The first time many businesses ever give serious thought to their trade secrets is when they find that they have been taken. It is then that the business begins scrambling to identify its trade secrets and, assuming it can put together a comprehensive list, hopes and prays that it has satisfied the requirements for keeping that information protected under the law of trade secrets so that it can use the legal process to keep it from being used by the businesses’ competitors. To make matters worse, when the disclosure of trade secrets is being threatened and an injunction from a court is all that will stop it, time is precious and every minutes can make the difference between winning or losing.

A business can be proactive by using this guide to prepare for the problem before it ever arises and, in doing so, help prevent the problem from ever arising. It can do this by: (1) carefully evaluating what information it has that qualifies as trade secret information; (2) implementing security measures, policies, and procedures to prevent the disclosure of that information and protect its trade secret status; and, (3) in the event its trade secrets are ever compromised, be much better prepared to quickly and efficiently make its case in a court of law and successfully prevent others from using its trade secrets.
What Are Trade Secrets?

Generally speaking, a trade secret is defined as any information that is valuable to a business and not known to others. Trade secrets are something unique about the way a business makes a product or provides a service that sets it apart from the competition. Because of this, trade secrets are a very important form of business information that are owned by the business; they fall within a category of property known as intellectual property.

For many businesses, their trade secrets are their most valuable asset. Trade secrets, however, must remain secret. If they become generally known they are no longer protectable as trade secrets and lose their value as the business loses its competitive advantage.

Trade Secrets As Defined By Texas Law

Texas’ definition of trade secrets comes from the Texas Uniform Trade Secrets Act (TUTSA), which became effective on September 1, 2013. TUTSA is Texas’ version of the Uniform Trade Secrets Act which has been adopted by 46 other states and Texas’ treatment of trade secrets will now be very similar to those other states.

Under TUTSA, a trade secret is information that meets two criteria. First, it is either valuable, or could be valuable, because it is not generally known to and cannot easily be discovered by proper means by competitors. Second, the business takes measures to keep that information secret that are considered reasonable under the circumstances.

TUTSA gives specific examples of the types of information that are considered to be trade secrets, but it is not an exclusive list: a formula, pattern, compilation, program, device, method, technique, process, financial data, or list of actual or potential customers or suppliers.

It is important to understand that the claimed trade secret cannot be obvious. That is, it cannot be something that someone could learn by looking at the product or service, or learn from reverse-engineering.
What Are Common Examples of Trade Secrets?

One way to help understand the definition of trade secret information is to consider some examples of commonly known trade secrets:

- The formula for Coca-Cola
- The formula for WD-40
- Google's search algorithm
- Kentucky Fried Chicken's secret 11 herbs and spices
- McDonald's secret sauce for the Big Mac
What Are Common Trade Secrets in Texas Businesses?

Here are common examples of the kind of information that many Texas businesses have developed and seek to protect as trade secrets:

- business plans
- business forecasts
- market analyses
- internal marketing plans and data
- budgets
- profit margin information
- customer and supplier lists and contact information
- specific information concerning customers and suppliers, including specifications and purchasing criteria
- confidential business relationships
- methods of calculating costs and pricing
- computer programs
- computer databases
- data compilations
- calculations and processes in computer programs
- research and development of future products and services
- confidential specifications
- confidential systems, processes, and methods
- formulas
- blue prints
- know-how and negative know-how (i.e., what doesn’t work, learned through trial and error)
Why Use This Guide?

What Are Trade Secrets?

What Are Common Examples of Trade Secrets?

What Are Common Trade Secrets in Texas Businesses?

What Are Your Businesses’ Trade Secrets?

What Are Common Threats to Trade Secrets?

How to Protect Your Businesses’ Trade Secrets

What If Someone Takes Your Businesses’ Trade Secrets?

Action Items!

What Are Your Businesses’ Trade Secrets?

Using the definitions and examples, consider the following questions with regard to your business:

1. What is it about your business that makes it unique and remarkable in comparison to your competitors?

2. Is there any information that is used for creating that uniqueness and remarkable?

3. What is it about your business and the way you do things that you do not want your competitors to learn?

4. What secret things that your business does would allow your competitors to do the same thing, the way yours does it?

5. What have you learned to not do in your business because you have found it does not work, but your competitors have not yet learned?

6. What confidential plans and preparations are you making to help your business?

7. Is there any other confidential information that makes your business more competitive that you want to keep confidential?

Write out everything you just thought of:
What Are Common Threats to Trade Secrets?

General Disclosure
Texas law says that a trade secret cannot be information that is generally known. If it is generally known, or becomes generally known, it cannot be a trade secret. There are very limited exceptions to this rule.

Trade secrets protection has been likened to a balloon that, once pricked with a pin, bursts and is gone forever. That is, once the trade secret information becomes generally known to the public, its trade secret status is burst and can never return.

The first major threat to trade secrets is any general disclosure of the information.

Internal Threats
People are the weakest link when it comes to protecting information. Statistics show that the vast majority of business information that is improperly disclosed or taken is done so by people within the business—insiders.

Internal threats can be either accidental or intentional.

Accidental Internal Threats
First, there are those people who are careless, negligent, or poorly trained and do things that accidentally lead to a disclosure of confidential business information. This often happens by clicking on email links, social media, or websites that are spear phishing attacks. Other times it is through simply talking too much and trusting others when they should not, whether at cocktail parties or in response to direct social engineering attacks. Finally, it can be losing a smart phone, leaving a thumb-drive, or losing a laptop with confidential information.
Intentional Internal Threats

Intentional internal threats come from an insider in your business who intentionally takes trade secret information which leads to its disclosure or use against you. A few of the reasons why they may do this is because they:

- contributed to the development of the information and believe they have a right to it
- want to keep a memoir of their work
- want to keep a copy for ideas in the future
- plan to use it to compete against you in the future
- have some ownership in the business and believe they have a right to it

Others may, with the best of intentions, store the information on personal devices or accounts while working for your business but later, once no longer working there, re-discover the information and decide to use or disclose it at that time.

Regardless of the reason, recent studies show that more than 60% of the insiders who leave a business take confidential information with them — oftentimes trade secret information — and many plan to use it to compete against the business.
External Threats

External threats can be either random or targeted.

Random External Threats

Random attacks can occur when your information is taken as part of a bigger criminal scheme such as a burglary in which files, data and equipment are stolen.

Random attacks are also how we would describe many hacking attacks, where hackers steal data from businesses without having any idea of what the data actually is and not knowing its value. A hacker’s goal is to penetrate your businesses’ computer system and then establish a connection between your system and theirs to use for exfiltrating data from your computer system. The data is usually packaged with other random data and sold in bulk on the black market (the Dark Net) much the way banks package bad debt to sell to debt collectors. The data is sold based on volume, not the value of its content, which is why your company’s data is just as valuable as anyone else’s for most random hacking attacks.

Targeted External Threats

Targeted external threats are those situations where someone who is not a part of your business specifically sets about to steal your businesses’ trade secrets. An example of this could be a burglar specifically targeting your business but, in reality, people have found that it is far more efficient to commit crimes using computers than crowbars. More often than not, when your business has information that someone else wants, they will take it with a smartphone camera, video, or directly through your computer system—not a busted out window. This is most common in corporate espionage cases where a competitor seeks to steal your businesses’ information but does not have someone on the inside to assist.
Blended Targeted Threats

Common threats in today’s highly-competitive business environment are blended targeted threats.

Departing Insider Leaving for a Competitor

The most common scenario is when an employee of your business is planning to go work for one of your competitors. Before resigning and while still in a position to have access to your businesses’ valuable trade secrets, that employee begins taking information and giving it to your competitor to undermine your business and give an unfair advantage to his future employer.

Disloyal Insider Planted for Corporate Espionage

A less common, but more egregious situation is where a competitor has a disloyal employee (or contractor, member of cleaning crew, etc.) planted as a trusted insider within your business and that person stays there, continuously providing a point of access to your computer system or directly exfiltrating your valuable information to the competitor over an extended period of time. The bigger problem with this is, when you are dealing with information, you cannot see it disappearing as you can with physical assets being stolen, and it can go on for years undetected. This is a classic example of corporate espionage. Not only are private businesses involved in this type of espionage but there are also many foreign state-sponsored corporate espionage operations directed toward American businesses.
How to Protect Your Businesses’ Trade Secrets

There are two important standards to consider for protecting your businesses’ trade secrets: (1) maintaining the legal protectability of the information as a trade secret, and (2) actually preventing the information from being obtained by anyone not authorized to have it. This guide focuses on the former—the legal protectability—as the latter is more a question of information security practices that are beyond the scope.

The Standards for Maintaining the Legal Protectability of Trade Secrets

Texas law requires that, to be protectable as a trade secret:

1) your businesses’ information is not generally known to, or readily ascertainable by your businesses’ competitors, and

2) your business makes reasonable efforts, under the circumstances, to maintain its secrecy.

What this really means is, if your business does not take seriously the protection of its claimed trade secret information, the law is not going to take it seriously either. The courts are not going to do your job for you.

Before the Texas Uniform Trade Secrets Act became effective, Texas law considered several factors in determining whether information was trade secrets, two of which focused directly on whether the information was adequately protected or easily discoverable. These two factors should still be considered by businesses seeking to protect trade secret information:

1) the extent to which it was known by employees and others involved in the business,

2) the ease or difficulty with which the information could be properly acquired, duplicated, or reverse-engineered.

As the courts decided cases that involved these factors, they began to look for some very specific things they would look for to see how
Why Use This Guide?

What Are Trade Secrets?

What Are Common Examples of Trade Secrets?

What Are Common Trade Secrets in Texas Businesses?

What Are Your Businesses’ Trade Secrets?

What Are Common Threats to Trade Secrets?

How to Protect Your Businesses’ Trade Secrets

What If Someone Takes Your Businesses’ Trade Secrets?

Action Items!

Businesses were handling the protection of their claimed trade secret information. These specific things will be integrated into the list of procedures that your business should consider doing with information it considers trade secrets, where it is practical.

3 Steps to Protect Your Businesses’ Trade Secrets

1. Obtain “Buy In” By Management and Employees to Foster a Culture of Information Security

No matter how well devised your plans may be, the most difficult part of any operation is the execution phase—that is, carrying out those plans. The most effective way to do this is by having strong “buy in” from your management team and employees.

People are inherently resistant to change. When that change requires more work and greater restrictions placed on them, they are even more resistant. Your strategic efforts can help.

First, you must explain the nature of the situation and help them understand that protecting the businesses’ trade secrets is vital to the health of the business and, therefore, their jobs. Without the business, they have no job; without the trade secrets, there is no business. This is something most people can understand.

Second, encourage them to think about the situation on their own and give you feedback on how they believe the businesses’ trade secrets could be better protected. If you take the time to discuss this with your people and you are genuine in seeking their feedback, you will be surprised at how thoughtful and perceptive they will be in pointing out ways that will help. Moreover, they will feel like they are part of the process and will be more receptive to the changes that will need to be implemented.

Third, train your people. Use practical scenarios to explain common situations that arise and encourage them to think through those scenarios conceptually. To think about the goal and to think about the various risks that threaten the businesses’ trade secrets. Train them on the policies and procedures that you implement.
2. **Promulgate Policies to Encourage Information Security**

Businesses generally need the following policies in place in order to adequately protect their trade secrets:

- **Non Disclosure Agreements.** NDA’s are the foundation for protecting trade secrets. Trade secret information can be disclosed to a person who has a legal obligation to maintain its confidentiality without the disclosure weakening its secrecy. NDA’s obligate the person receiving the information to maintain its confidentiality.

- **Policy Manuals.** Businesses should have Policy Manuals that:
  - explain the need to protect the businesses’ information; require employees to maintain confidentiality of such information;
  - explain that its computer systems and data are owned exclusively by the business and their use is authorized for business purposes only; explain that any access to or use of such computer systems or data for any non-business purpose is unauthorized and may be prosecuted under law; notify that the use of those systems may be monitored; prohibit the transmission or storage of the businesses’ data to unauthorized devices or services; and require disclosure of any compromise or breach of system or data security.

- **Intended Use Policy.** Most people refer to this as an Acceptable Use Policy but I have a reason for calling it this. Trust me. Regardless of the name, the purpose of the policy is to specifically define and limit exactly what can and cannot be done with the businesses’ computer system and data, in greater detail than the Policy Manual.

- **Computer Login Screens.** These require employees to abide by all restrictions and certify that they are not accessing the system or information for any non business purpose.

- **Non Compete Agreements.** When employees are provided with unique training or access to trade secrets and other proprietary information to perform their job, your business should require them to enter into a Non Disclosure and Non Compete Agreement to help keep them from taking that knowledge or information and using it to compete against your business.
3. Implement Procedures to Encourage Information Security

You should consider implementing the following procedures, as appropriate for your business. Remember, the standard is what is reasonable under the circumstances. Some situations may require an extremely high level of protection, others may not. Each situation is different.

- require NDA’s for every person having access to trade secrets or to whom trade secrets are disclosed or discussed—no exceptions
- keep a record and copy of all NDA’s
- carefully vet and perform background checks on all people who have access to trade secrets
- continue to monitor the personality, behavior, and work habits of all employees who have access to trade secrets
- limit access to only those people who have a need-to-know trade secrets and terminate access when no longer necessary
- use technological restrictions and access controls to ensure that non need-to-know insiders do not have access to the information
- monitor and log all accesses to the trade secrets
- have system alerts for unauthorized internal and external access
- disable USB ports to prevent downloading data to thumb-drives
- disable or monitor usage of cloud storage services
- maintain adequate physical security of the premises and all network servers
- mark the information as “confidential”
- for extremely sensitive information, consider
  - storing it on a computer that has no connection to the business network or the Internet
  - limiting access to that computer to only absolutely necessary personnel
  - carefully vet and require security clearances of those personnel
  - encrypt the data on a file-level basis
What if Someone Takes Your Businesses’ Trade Secrets?

Under Texas law the taking of trade secret information is called a misappropriation. A misappropriation can be a taking or a disclosing of a trade secret without permission, as well as having or using a trade secret with knowledge that it was wrongfully taken.

You have 3 years from the date of the misappropriation to bring a lawsuit for misappropriation of trade secrets. Misappropriation of trade secrets is a claim that arises under the state law of Texas and, therefore, is usually brought in the county or district courts in the state of Texas. A successful claim for misappropriation of trade secrets may entitle you to recover damages and, in some cases, exemplary damages, and attorneys’ fees.

Emergency Situations—Injunctions to Prevent Disclosure or Use

When someone is threatening to misappropriate, disclose, or use your businesses’ trade secrets, you must ensure that they are stopped from doing so immediately. Texas law permits the owner of the trade secret to seek an injunction that will prohibit the use or disclosure of the trade secrets, as well as take affirmative steps to protect the confidentiality of the trade secrets.

In these situations, time is of the essence and every second counts. Once the trade secret information is disclosed to the world—such as over the Internet—it is like the balloon pricked by the pin. It is gone.
Action Items!

The importance of being prepared cannot be overstated. It is vital to the overall odds of your businesses’ ultimate success or failure in protecting its trade secrets. That is why it is important to be proactive and get prepared now by taking these four steps:

1) Use this guide to start developing a basic understanding of what your businesses’ trade secrets are and begin thinking of some of the ways that would work best for protecting them;

2) Contact a lawyer who is experienced with trade secrets to develop a specific set of policies and procedures, then implement them;

3) Work with your IT department or service provider to evaluate the security of your computer system and implement necessary changes;

4) Follow the recommendations in this guide and from the attorney to ensure that your trade secrets are protected.

For more information, please contact:

Shawn E. Tuma
214.472.2135
shawn.tuma@solidcounsel.com

©2015 Shawn E. Tuma. All rights reserved. This publication is intended for general information purposes only and does not constitute legal advice. Because the facts and circumstances of each case are different and the laws may have changed since the time this publication was written, the reader should consult with legal counsel to assist in applying the general information provided herein.

ATTORNEY ADVERTISING