Trade Secret

The Q and A of Intellectual Property
Presented by:
What Is a Trade Secret?
The federal Defend Trade Secrets Act (DTSA) defines a trade secret as “all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled or memorialized physically, electronically, graphically, photographically, or in writing.” In order for information to qualify as a trade secret, you must take reasonable measures to maintain the secrecy of the information, and it must also be of economic value to your competitors. In other words, a trade secret is typically something that is not publicly known and that gives your business a competitive advantage.

What Constitutes Misappropriation?
In order to prove misappropriation of a trade secret, you must prove not only that the information at issue meets the legal definition of a trade secret but also that it was wrongfully obtained by the accused party. The Uniform Trade Secrets Act (UTSA) includes a lengthy definition of “misappropriation,” which boils down to (i) acquisition of a trade secret by a person who knows or has reason to know that the trade secret was acquired by improper means or (ii) disclosure or use of a trade secret of another without express or implied consent by a person who used improper means to acquire knowledge of the trade secret. Misappropriation of trade secrets claims are often accompanied by breach of contract claims—breach of confidentiality or nondisclosure agreements being the most common among them. Confidentiality provisions are routinely included in a whole host of commercial contracts, including employment agreements, manufacturing agreements, distribution agreements, and supply agreements.

Are Trademark Secrets Protected by Federal or State Law?
Trade secrets are protected by state and federal law. Until recently, trade secrets were only protected by state law; however, in 2016, Congress enacted the Defend Trade Secrets Act, which establishes a federal case of action for misappropriation of trade secrets. The federal act provides an ex parte seizure remedy, which gives courts the authority to issue seizure orders for stolen trade secrets without hearing from the defendant. Federal law also provides immunity to whistleblowers who disclose trade secrets to attorneys and government officials “solely for the purpose of reporting or investigating a suspected violation of law.”

The Uniform Trade Secrets Act has been adopted in nearly every state, including Montana. The definitions of “trade secret” and “misappropriation” are largely the same under the UTSA and the DTSA, but the DTSA expressly excludes “reverse engineering, independent derivation, or any other lawful means of acquisition” from the definition of misappropriation.

What Are Examples of Trade Secrets?
A trade secret includes anything that would be of value to a competitor, for example, manufacturing processes, scientific formulations, and computer source code. It may also be something as mundane as how much you pay your employees, who your suppliers are, and the terms and conditions of your customer agreements. The Google search algorithm and Coca-Cola’s recipe for its signature beverage are two common examples of trade secrets.
How Small Businesses Are Infected

Ransomware is a form of malware that encrypts a victim's information and holds it for ransom. It is often designed to spread across a network and target all critical information, and can quickly paralyze an entire small business. It is a growing threat, generating billions of dollars in payments to cybercriminals and inflicting significant damage and expenses for businesses and governmental organizations.

How To Protect Your Small Business

Phishing

Clicking on links or opening attachments from attackers in emails.

Unsecure Websites

Visiting nonsecure, compromised websites can download malware.

Outdated Software

Old, unmaintained software may have vulnerabilities attackers can leverage.

The Typical Attack Process

1. Cyber criminals gain admin access using above attacks
2. Your network is explored to locate and steal critical data
3. All backups and protections are destroyed
4. All data is encrypted and you are locked out
5. A ransom request is sent, with offer to unlock data
6. Cyber criminal receives ransom or data is published

Backups -

If your data has been encrypted and your backups are deleted, you are left with few choices. Paying the ransom and getting the key does not guarantee that your data remains intact and usable. Make your own encrypted backups daily. Consider how to isolate them to prevent deletion or destruction.

Sensitive Data -

Understanding what data you collect is just as important as protecting it. Determine if you actually need to collect all the data you have. Then make sure the data is encrypted and access to that data is tracked.

Network Segmentation -

Nothing makes an attacker's job easier than a network where every system is accessible with one login, and there isn't any internal monitoring. Make sure you setup a network where only the systems that need to talk to each other are connected. Placing firewalls around critical data can help protect it from unwanted visitors.

Access Control -

When an attacker gains access to your network, their primary goal is to gain administrative access to all systems. Typically the bulk of their work is performed in a semi-automated fashion using special programs that require administrative rights. Adding Multi Factor Authentication administrator logins can slow or stop their efforts.

Patching & Updating -

When a new update is released for software that patches a vulnerability, attackers immediately begin scanning the internet for vulnerable systems to exploit. While it may not be practical to patch instantly when an update is released, timely updates can reduce the chances of your system being compromised.

Is There a Registration Process for Trade Secrets?

No. There is no registration process for trade secrets. In order to protect something as a trade secret, you must have appropriate confidentiality agreements in place with everyone (including employees, vendors, manufacturers, etc.) who has access to the trade secret, and you must also restrict access — physically or electronically, depending on the nature of the trade secret — to the information that you are claiming is a trade secret. For example, if the trade secret is a manufacturing process, then you would require anyone visiting your factory to sign a written confidentiality agreement, and you would not show them certain highly confidential aspects of your operation. Because there is no registration process for a trade secret, there is no definitive way to determine in advance of litigation whether something is or is not a trade secret.

Although there is no international registration system for trade secrets, the World Trade Organization’s General Agreement Tariffs and Trade 1947 (the “TRIPs Agreement”) officially recognizes trade secrets as a protectable form of intellectual property and requires member states (countries) to adopt certain substantive and procedural protections for trade secrets.