COMMON SITUATIONS THAT PUT YOUR TRADE SECRETS AT RISK

SCENARIO 1: YOUR EMPLOYEE IS LEAVING

In some situations, there's a fine line between general skills and knowledge and trade secrets when it comes to your employees. Some information, like trends in customer preferences the employee noticed while working with your company, may not be deemed trade secrets. But, there's no doubt that when employees leave, your trade secrets are at risk.

SCENARIO 2: THROUGH THIRD PARTY RELATIONSHIPS

When you share confidential information with a third party – be it a manufacturer, a software provider, a marketing agency, or a joint venture partner – you are extending the circle of people who know your secrets. Despite documents that are intended to prevent disclosure of confidential information, the more people that have access to your trade secrets, the more risk you face.

SCENARIO 3: CYBER ATTACKS AND DATA BREACHES

Cybercrime has never just been about stealing consumer data. There's an entire realm of threat actors who target confidential information and trade secrets for their economic advantage.

You may remember the very high profile theft of Volvo's R&D during a cyberattack in 2021. That's an example of how cyber attacks and data breaches can impact your trade secrets.

A FRAMEWORK FOR MAINTAINING TRADE SECRETS

Step 1: Identify and Clearly Define Your Trade Secrets

You can't protect what you haven't identified as a trade secret. So step one requires you to conduct a thorough audit. Consider and document:

- What information gives you a competitive edge? Be specific. Is it the precise temperature and timing for a chemical process? The algorithm that powers your recommendation engine? The detailed demographic data of your most profitable customers?
- How important it it? Is it mission-critical, nice-to-have, or readily replaceable? You may find that some of what you're keeping secret isn't sufficiently valuable to justify the effort needed to protect it.
- Where is this information located? Is it in documents, databases, code repositories, physical blueprints, or someone's head?

THE TAKEAWAY: CLEARLY DOCUMENT WHAT YOUR TRADE SECRETS ARE, HOW THEY PROVIDE VALUE, AND YOUR EFFORTS TO KEEP THEM SECRET.

A FRAMEWORK FOR MAINTAINING TRADE SECRETS

Step 2: Introduce Adequate Protections

Once you know what you're protecting, you need to put up defenses. This may involve legal, physical, technical, or procedural safeguards, or a combination of two or more mechanisms.
In terms of legal protections, you'll want to employ confidentiality agreements as well as clear company policies.

Confidentiality agreements (also known as Non-Disclosure Agreements/NDAs) should be signed by every employee, contractor and consultant who could be encountering proprietary information, as well as business partners and vendors – even during the preliminary phases of a business relationship if you might need to share trade secrets with them down the line.
These agreements must identify with particularity what is to be considered confidential information that's within the scope of the agreement. They can be standardized for your company, but be aware that they may cover different types of information and could impose differing obligations on one set of parties vs others.

QUICK TIP: A BEST PRACTICE IS TO MARK OR OTHERWISE TAG DOCUMENTS AND DIGITAL FILES AS CONFIDENTIAL TO HELP YOUR EMPLOYEES AND THIRD PARTIES IDENTIFY IT.

A FRAMEWORK FOR MAINTAINING TRADE SECRETS

Step 3: Monitor and Detect

Security provisions aren't enough. You must also have measures in place to detect (and ideally prevent) potential theft or disclosure in a timely manner.

Consider:

- Network Monitoring: Monitor network traffic for unusual activity, such as large data transfers to external storage devices or personal cloud accounts, access to sensitive files by employees who don't typically need them, or access at strange hours.
- Endpoint Monitoring: Tools can monitor activity on employee computers, including file access, downloads, and attempts to print or email sensitive documents.
- Insider Threat Programs: Develop a program to identify potential insider threats. This involves behavioral analysis, monitoring access patterns, and creating a culture where employees feel comfortable reporting suspicious activity (with appropriate whistleblower protections).
- Monitoring Public Sources: Keep an eye on public information, competitor activities, and online forums for any signs that your trade secrets may have been disclosed.

Need Help Managing Your Company's IP? Reach out.

Your trade secrets often represent the culmination of years of innovation, investment, and hard work. As such, they make your business work more productively, efficiently, and successfully. They're worth protecting.

By using this three-step framework, you should be well placed to prevent many instances of trade secret misappropriation and misuse, and to defend your company's control over its confidential information in case it is misappropriated.

If you need assistance managing your company's IP assets and agreements, reach out. Our team of intellectual property attorneys is ready to work with you.

NOAM COHEN
CO-FOUNDER AT CGL

HANNAH GENTON
CO-FOUNDER AT CGL

CGL-LLP.COM