Expert Tips and Rookie Mistakes When Implementing a Trade Secret Protection Plan

Every business has proprietary trade secrets that give it a competitive advantage. A trade secret is confidential, commercially value information that has economic value and that the business is making a commercially reasonable effort to guard the secrecy of the information. Trade secrets can include business information and data such as business and marketing plans, financial records, proprietary processes, customer and vendor lists, and new product concepts. Business owners should take affirmative steps to protect proprietary information from being disclosed to or used by others.

There is no limit to the length of time your company can maintain a trade secret. Some well-known companies have maintained trade secrets for more than a century. The key was extremely limited access to the information to the fewest people possible and on a need-to-know basis only.

Protecting trade secrets is a continuing process for a business owner. The extent of security measures should be in alignment with the value of the information being protected. The more valuable the information, the greater efforts the business will be expected to take to protect it. If the business itself does not take reasonable efforts to protect the information, the courts will consider that when evaluating claims of misappropriation.

It starts with identifying trade secrets in your business and appointing someone to be in charge of the overall trade secret protection plan. Business owners should implement physical security by setting up protocols for visitors, restricting access, and where appropriate, using video surveillance and security monitoring. They should also implement cybersecurity measures such as limiting computer access (passwords and administrative rights), preventing copying of sensitive information on personal devices, monitoring emails and remote access, and keeping computer event logs.

The business should also educate executives, employees, and contractors on what is subject to trade secret protection, their role in protecting the business' proprietary information and the plan for reporting and responding to incidents. The business should also ensure that any new hires are not subject to any NDAs or non-competes that could impede their ability to work for the business or subject the business to liability for trade secret misappropriation. A signed statement during the new hire onboarding process is generally the easiest way to accomplish this objective.

Confidentiality agreements, also called non-disclosure agreements or NDAs, are legally binding contracts where a party agrees not to disclose or use confidential information (except for the business' own purposes) for a stated period. Confidentiality agreements should be signed by key employees, vendors and contractors (executives, consultants, subcontractors, R&D people, salespeople and others with access to sensitive information). The agreements should be as specific as possible about what is deemed confidential information and be time limited. Courts will limit the scope of any associated non-compete to what is minimally necessary to protect the

business' legitimate interests without restricting the ability of employees and contractors to seek gainful employment. Exit interviews should reinforce and remind departing employees of their obligations of confidentiality of trade secrets they learned during their work with the company.

The business' NDAs should be reviewed to identify any steps that need to be taken to protect confidential information. Often they require documents be marked as "confidential' or that oral conversations be memorialized in writing, Failure to adhere to the process set forth in the NDA can be fatal to protecting the confidential information as a trade secret. When a project ends, it is also a best practice to request return or destruction of any trade secret information that was given to the other party over the course of the business relationship. This will ensure it does not end up in the wrong hands down the road.

The last tidbit I'd like to leave you with today is that it is not a violation of trade secret law for someone to independently develop the same information, to learn it from a separate and legitimate source, or to reverse engineer a product. They can't steal your confidential information, but they can develop their own as long as they don't use yours in the process. Most people are surprised to learn that reverse engineering is perfectly legal as long as there is not contractual obligation forbidding such practice (some NDAs do contain such clauses).

Take-aways- your checklist of to-do's

1. Be sure you obtain copyright assignments for any creative content prepared by others, especially for logos and other trademarks
2. Be sure you use work for hire agreements for future creative content prepared by others and consider having a trademark clearance search on any newly created brand logos and trade names
3. Review your website to ensure it has a privacy policy, terms and conditions, DMCA notice and is ADA compliant
4. Review your website and written materials to be sure you have properly used copyright and trademark notices where appropriate
5. Be sure to use NDAs to protect the business' proprietary trade secrets
6. Review your business to identify its valuable and key trade secrets and develop a plan to protect them and monitor for misappropriation
7. Review documents that list your pricing to ensure it includes any credit card charges