Protecting Trade Secrets

Jason Balich ▪ Wolf Greenfield

Companies increasingly protect their innovative technology as trade secrets instead of patenting them, which makes sense in many circumstances. For example, patents expire after twenty years, but trade secrets can last forever. However, safeguarding trade secrets presents unique challenges in an increasingly interconnected and data-driven world. While trade secret law only requires "reasonable measures of protection," protecting trade secrets in practice requires establishing a plan to ensure that your company's trade secrets are protected now and forever.

Establish a confidentiality plan. Start by creating a plan that defines what confidential information, including trade secrets, your company needs to share and with whom. This plan should outline how the information will be used and the protections for handling it. Limiting disclosure is essential; only disclose what is necessary for a specific business purpose. For example, Coca-Cola's success in keeping its formula a trade secret stems from highly restrictive disclosure policies. This approach minimizes risk by ensuring that only a few individuals have access to vital information.

Furthermore, consider limiting what information your company accepts from others. Taking on sensitive information from outside sources can limit your company's ability to develop and monetize similar innovations independently. Sequestering external confidential information with a designated employee (separate from product development teams) and maintaining a detailed log of any received information are best practices that help mitigate these risks.

Use non-disclosure agreements (NDAs). Keeping information secret usually starts with executing an NDA that formalizes the responsibilities of and restrictions placed on the recipient of confidential information. Consider the following types of covenants when drafting any NDA:

• *Marking.* NDAs should define what is confidential and how it should be identified. One approach is to define any non-public information as confidential, but this places a heavy burden on the recipient to differentiate confidential from public information. Another approach requires the disclosing party to mark confidential information as such — for example, by labeling documents. That approach takes the guess work out of the equation for the recipient but puts the burden on the owner of the information.

• *Ownership.* NDAs should address who owns new ideas developed using disclosed information to avoid future disputes.

• *Term of disclosure and protection.* The NDA should specify the length of time that information will be exchanged and the length of time it needs to be protected. While business information often becomes stale after a few years, trade secrets require protection for as long as the information qualifies as such.

Establish reasonable measures of protection. Any confidentiality plan should consider other measures beyond NDAs to protect trade secrets:

• *Secure storage.* Trade secrets should be stored securely, both digitally and physically. For electronic storage, use encryption, password protection, and logging of user access. Physical storage should be secured with locks and controlled access.

• *Documentation and logging.* Maintain detailed logs of all exchanges of trade secrets, including the date, recipient, and type of information shared. This record helps to verify the history of disclosures if disputes arise.

• *Limit access.* Restrict the number of employees with access to sensitive information to minimize potential exposure. Unauthorized or widespread access increases the chance of inadvertent disclosures.

• *Training.* Conduct training sessions to educate employees on confidentiality policies, and document their participation. At employee exit interviews, remind departing employees of their confidentiality obligations, retrieve all company property, and monitor for any potential misuse of confidential information.

• *Audits.* To ensure adherence to confidentiality protocols, conduct internal audits. For external parties, demand the right to audit compliance to verify adherence to agreed-upon security practices.

Follow up at the end of any relationship. When a relationship ends with another company or an employee, remind parties of their confidentiality obligations. Your company should ensure that any NDA's terms regarding the return or destruction of confidential materials are followed. A detailed log of what was shared can streamline this process to ensure that all information is accounted for. You should destroy information received from other parties and document that destruction as a safeguard against accusations of misappropriation in the future.

Consistency is key. While not all of the above measures apply in every situation, each should be considered. A proactive approach to maintaining trade secrets balances business needs with security. Once the right balance is struck and a plan has been put in place, consistency becomes key. Consistent follow-through helps to safeguard a company's trade secrets in perpetuity. CEP

Jason Balich is a trial and appellate lawyer at the law firm Wolf Greenfield, based in Boston, MA, where he protects clients' technology and defends their freedom to use it. He has a BSE in chemical engineering from Princeton Univ., an MBA from Bentley Univ., and a JD from Quinnipiac Univ. School of Law.