Insider Threat

Employees Responsible for 85% of Trade Secret Theft

TRADE SECRET theft by employees is a serious and growing problem in the U.S. According to an analysis of federal court cases, 85% of such theft is committed by employees or business partners.

Lately, companies have been focusing on high-value, high-tech cyber attacks by outsiders that breach databases, but threats from the inside are just as costly. Despite that, a survey by PricewaterhouseCoopers found that only 49% of organizations surveyed had a plan for responding to insider threats.

Trade secrets are particularly susceptible to theft because they consist of protected information with economic value. Company insiders often find that information too tempting to leave behind when changing employers, or when seeking new employment.

That could lead to a former employee leaking that info to their new employer or using it in other ways to the detriment of their prior employer.

Protect Company Secrets from Internal Misuse

- **Identify your secrets** – In order to protect your trade secrets, you need to know what they are and where you store them. Broadly speaking, any confidential business information which provides an enterprise a competitive edge may be considered a trade secret. Trade secrets encompass manufacturing or industrial secrets and commercial secrets. Legally, you should know that different states define trade secrets differently, so you should familiarize yourself with California's definition.
- **Limit access** – Restrict trade secret access to those who have a need to know. Have these employees sign a confidentiality agreement in which they:
  - » Acknowledge receipt of confidential material.
  - » Agree to keep the material confidential.
  - » Agree to return the material when employment ends.
  - » Agree to advise you of the identity of their new employer and to make the new employer aware of the agreement.
  - » Agree to allow you to provide a copy of their agreement to a new employer.
  - » Acknowledge that forensic analysis may be done on their devices, such as computers and phones, when their employment ends.
  - » Acknowledge that irreparable harm would be done if they violate it.
- **Use non-disclosure agreements** – Have employees who have access to your trade secrets and customer information sign non-disclosure agreements. You can customize the agreement to ensure it reflects the worker's role in the company, so you have a better chance of enforcing the agreement should it be breached. Do not use a "one-size-fits-all" form and don't have workers sign such agreements when there is no legitimate business reason.
- During employee meetings, regularly address the importance of keeping information confidential. This will convey that you are serious about safeguarding your company information, particularly when an employee leaves the company.
- Conduct exit interviews with employees who had access to trade secrets and:
  - » Confirm in writing the obligations the employee has by contract, or otherwise by law, to keep confidential information confidential and, if applicable, not to compete or solicit.
  - » Confirm that all confidential material has been returned.
  - » Inquire about the person's next job.
- Perform forensic analysis on computers and other devices of departed workers who had access to trade secrets to determine whether any thievery of trade secrets or other prohibited conduct occurred.

The takeaway

While the above steps are not foolproof, they can go a long way towards protecting your company's trade secrets. And if an employee or departing worker makes off with any of this data, you will be in a better position to minimize and mitigate any harm that may come from it. ❖