MAY 15, 2025 | AI/TECHNOLOGY, PRIVACY & DATA SECURITY

Best Practices to Safeguard Your Company's Trade Secrets — Case Study

BY JORDAN B. SCHWARTZ

By Jordan Schwartz

The number one risk for trade secrets exfiltration is from insider threats—employees, contractors, or even executives with access to sensitive information who either intentionally or accidentally compromise it. Sometimes it's malicious, other times, it's accidental; like emailing a client list to a personal account for convenience. Regardless of the intent, however, your company must put itself in the best possible position to protect against the exfiltration of its trade secrets and confidential and/or proprietary information. Otherwise, your company could suffer extreme financial damage and, perhaps even worse, lose its competitive edge in the marketplace. To explain this point further, I present you with the following case study:

We represent a company that has invested considerable time, effort, and expense to acquire, aggregate, and analyze various operational processes and structures to provide the highest quality services for its customers. Like many companies, its success depends on all kinds of confidential information with respect to its operations, including products, pricing, standard operational processes, key performance indicators, and training strategies, as well as the maintenance of such confidential information. As a result, before it provides certain employees with access to its confidential information, the company requires them to sign a confidentiality agreement as a condition of employment.

1. Companies should identify, catalog, and regularly audit their trade secret information.

One of the biggest mistakes companies make is assuming everyone knows what needs to be protected. Trade secrets are often buried in day-to-day operations and overlooked. Moreover, security is not just a technological problem; it is a people and process issue too. Thus, company executives should think about their business' most valuable processes, formulas, and relationships and then ask: who has access, who tracks that access, and how is it stored? A company needs systems that not only protect information but also make employees aware of the type of information that is sensitive (and worth being protected). After a company answers these questions, it can then implement classification, tracking and security protocols, and disseminate appropriate policies. And don't forget about what happens after information is no longer needed, as poor document disposal procedures is one of the easiest ways to lose control of sensitive data.

2. Companies should provide consistent, periodic training on handling confidential information and trade

secrets.

Such training could include (i) terms of use for devices, systems, data, access; (ii) the appropriate use of non-disclosure agreements and/or restrictive covenants; (iii) assignment agreements; and (iv) security awareness training. Indeed, employees cannot protect what they do not know is confidential (or choose not to know is confidential). Regular, ongoing training (e.g., not just training for new hires) ensures that employees understand what is sensitive and how to handle it; it also helps reinforce expectations and keeps security top of mind, as it is important to connect policies to real-world risks so your workforce knows why it matters, not just what the rules say. To put it succinctly, when employees are trained well, they become an active part of your protection strategy, not just potential sources of risk.

3. Companies need to keep a close eye on the behavior of their employees, as many red flags are personal and behavioral, which are things that can and should be noticed long before information is compromised.

For example, a disgruntled employee or someone with a poor performance record may be more likely to act out or mishandle sensitive info. You also want to keep an eye out for folks who think the rules don't apply to them (i.e. an "above the rules" attitude). When someone bypasses their supervisor or goes directly to leadership, it may indicate conflict or a lack of trust. Likewise, repeated security violations, or odd work patterns like showing up late at night or on weekends, may indicate concerning behavior. Finally, someone who frequently expresses that they are underappreciated could be at higher risk for trade secret theft.

4. Companies should monitor digital activity as much as is practicable. While personal behaviors can raise red flags, technology often tells the real story.

Digital activity typically leaves a trail and with the right monitoring in place, it can give you an early warning before a breach occurs. Sudden changes in email use, access patterns, or device use all could be indicators of trade secret theft. The key is having monitoring systems in place that do not just collect data but flag and review suspicious activity in real time, especially since a company's highest risk window is right before or right after someone leaves the organization. Companies should have robust policies in place preventing employees from sending company-related information to their personal email accounts and from being able to download documents to a USB device; companies also may want to monitor employee emails to make sure such activity does not occur. While this type of conduct may be the result of a careless employee with no ill intentions as easily as a malevolent employee who wants to harm the company, from the standpoint of protecting your company's confidential information, both situations are risky and could lead to the exfiltration of sensitive data. Accordingly, prior to the termination of an employee, a company should review that employee's email history and take steps to recover any and all emails sent to their personal email address, especially if any of those emails contain confidential or proprietary information or trade secrets.

5. It is important not to overlook physical security, as that is often where digital protection breaks down.

Depending on your industry and/or what is being made at your physical place of business, your company may want to control who can enter sensitive areas, whether through badges, locked doors, or clear visitor protocols, and restrict recording or photographic devices in areas with sensitive information. Likewise, companies may want to track the movement of certain employees, as logs, video surveillance, cameras, and ID systems can help

identify unusual access patterns. Companies should also mark and monitor their most sensitive physical documents and be sure they are stored securely and disposed of properly. Companies should empower employees to speak up if they see suspicious behavior on-site and even have a suspicious behavior reporting system in place, if possible.

6. Every company should have a clear plan for managing trade secret exfiltration, especially during periods of employee transitions or potential insider threats.

Finally, your company should plan and roadmap for onboarding and offboarding, including plans for responding to a potential insider threat incident. Departing employees are one of the most common sources of trade secret exposure and one of the most preventable. As a result, your company should routinely conduct entry and exit interviews and have a clear plan for how to handle employee terminations. The exit process should be thorough, not rushed, and should include the company recovering all devices, removing access to those devices, and having an in-person conversation about continuing confidentiality obligations. Your company should pay special attention to digital access, as cloud tools, shared folders, or auto-saved credentials can be easy to overlook. Importantly, as with our case example, do not assume that the company-issued technology will be returned in clean condition. Accordingly, make sure to secure the hardware and keep a chain of custody. A final inventory helps ensure nothing walks out the door, either physically or digitally.

It is important to keep in mind that it is not a one-time project to implement the strategies set forth above. Trade secret protection is something you and your company must continually revisit as your business grows, your team changes, and new tools or platforms are introduced. Nevertheless, keeping these strategies top of mind will go a long way in allowing you to rest a little easier knowing that your company's trade secrets and confidential and proprietary information are sufficiently protected.