The Anatomy of a Trade Secret Audit to Protect IP

Corporate, Securities, and Governance

CHEAT SHEET

- ***Begin at the beginning.*** Protecting trade secrets should begin during the onboarding process as disgruntled employees are often the biggest threat to companies.
- ***Information security policy.*** Companies should develop an information security policy that identifies what is considered a trade secret and how employees should treat and protect this information.
- ***Security measures.*** During a trade secret audit, organizations should review their security measures — physical security, data security, legal reviews, third-party access, password protocols, and systems monitoring.
- ***Trade secret protection plan.*** After the audit, the company should implement a formal trade secret protection plan that includes procedures to prohibit disclosure of trade secrets, appoints those responsible for the plan, outlines employee protocols, and incorporates future audits.

Trade secret theft has increased in recent years with greater employee mobility between companies, the alarming frequency of targeted data thefts, the pervasive use of mobile devices as a primary tool for conducting business, and the explosion of social media and cloud computing. Companies must be proactive to protect trade secrets; They cannot simply react to these real business risks after the data has been compromised. By then, it’s too late.

In-house protection mechanisms

As in-house counsel, you should ensure that protection mechanisms are in place that follow the employee lifecycle.

INCOMING CANDIDATES:

- Perform background checks and reference checks
- Ensure your talent acquisition team has a firm grasp on the forms and policies they need to supply to new hires (including global variations)
- Adequately document employee non-disclosure and protection of trade secret obligations in the onboarding documentation (this is typically achieved by requiring new employees to execute appropriate confidentiality and restrictive covenant agreements)
- Incoming employees should be reminded not to bring or use any prior employer's confidential information or trade secrets

CURRENT EMPLOYEES:

- Provide periodic trainings regarding the protection of company confidential information and trade secrets
- Require periodic certifications and policy acknowledgements
- Supply updated restrictive covenant agreements when necessary (be aware of state laws regarding adequate consideration in exchange for signature)
- Agreements should be updated and compliant with relevant state law. No in-house lawyer wants to have to inform the executive team that the agreement you have in place with an employee cannot be relied upon due to enforceability issues under relevant state or jurisdictional law

EXITING EMPLOYEES:

- HR should remind exiting employees of their contractual post-separation obligations
- Access rights to company systems and confidential information should be shut down immediately upon (or just prior to) separation depending on the situation at hand

While companies can certainly protect some of their assets with traditional methods of IP protection like patents, trademarks, and copyrights, there is still a treasure trove of other important company information that would qualify as a trade secret under state and federal law now that the Defend Trade Secrets Act (DTSA) has passed, provided that information has an independent economic value and is properly safeguarded by the company. Additionally, given recent changes in the patent laws, trade secret protection can provide protections where patent laws no longer may. Indeed, trade secret protection can provide another and sometimes the sole layer of protection if the intellectual property does not qualify for trademark, patent, or copyright status. As a result, preserving trade secret status is absolutely critical. You cannot close the Pandora's box of trade secrets after you have opened it; once the trade secret is disclosed, it's gone.

Registering trademark, copyright, and patents with the government, and complying with the statutory

guidelines, automatically activate IP protections. However, there is no government registration or review of trade secrets. State statutes, the DTSA, and case law interpreting those statutes define what is, and what is not, a trade secret, but there is no guarantee that your information will be deemed a trade secret until a dispute arises and you commence litigation. Most commonly, this arises when your company is either suing a former employee, consultant, vendor, or some other individual or entity for stealing a trade secret, or your company is defending a suit from a competitor alleging that you have either conspired with a newly hired employee to steal the former employer's trade secret or that your company has taken them directly. Your company will need to demonstrate during the early stages of these disputes not only that a "trade secret" is involved, but that the company has taken reasonable measures to keep such information "secret," the information derives independent economic value, actual or potential, and further that it is not generally known to the public or readily ascertainable.

With traditional IP protections in place, you may ask yourself, why is protecting trade secrets so important? Trade secrets are frequently a primary driver of company success and are often the lifeblood of the company. Recent headlines remind us that companies have lost billions of dollars from theft of their proprietary information. Public companies that do not protect their trade secrets can face shareholder suits. On the other end of the spectrum, startups may never get off the ground if they are not able to demonstrate that their trade secrets are secure as investors will not tolerate absent assurances that protection programs are in place.

Companies are often so consumed with the possibility that their IP will be compromised through external threats that they fail to recognize that the biggest threat to their trade secrets is often their own employee base — particularly disgruntled employees. After all, who is in a better position to understand what types of information the company deems important and how to access that information? That type of inside knowledge is exactly why companies need to take a proactive approach to protection of trade secrets. This proactive process can and should start at the onboarding process with your recruiting/talent acquisition team and continue through the employee life cycle.

Companies need to analyze existing IP and the protections needed to better protect trade secrets in the courts. This is where a trade secret audit is imperative. The mere fact that a company has conducted a trade secret audit will be valuable evidence in later litigation. The company will be able to show that it has undertaken reasonable measures both to protect the secrecy of its proprietary information and also to prevent the improper use of trade secret information brought to the company by new employees, vendors, or others. There are risks, however, associated with conducting an audit, including the risk that weaknesses in the company's treatment of trade secrets will be exposed. For this reason, audits should be conducted under the supervision of counsel to protect the audit under attorney-client privilege and shared only with those who must act on the findings. Special care must be taken to avoid waiver of the attorney-client privilege by copying counsel on communications and making sure that those with access to the information don't disclose it to others outside of attorney-client communications.

Monitoring changes in the law

This is a critical element in the protection of trade secrets and enforcement of your restrictive covenant agreements. If your agreements are outdated and challenged in court, in some states you risk not just the unenforceability of a specific clause within the agreement, but possibly the agreement in its entirety. This can put the company at significant risk. For that reason, monitoring changes in the

law and periodically reviewing your agreements with outside counsel in light of material changes in the law is a good practice to follow.

In light of the very real risks trade secret violations pose for companies, this article provides a suggested eight step process for in-house legal teams and their business clients to follow in order to protect a company's most important assets. These steps will help effectively manage risk by conducting trade secret audits on a regular basis to ensure adequate protections are in place to minimize the risk of theft.

Suggested steps for an audit:

1. Create a project plan.

Before you commence the audit, it is prudent to develop a comprehensive plan for the audit, including the audit's scope and a timeline of steps. As part of the plan, determine whether the audit will be aimed at one arm of the company or the entire organization. It may make sense to start in one segment of the business and then expand beyond that once the first segment is complete. If your organization has project management resources, consider enlisting a project manager to keep the audit on track, help catalogue the trade secrets identified, and ensure that recommended action items are addressed.

With respect to cataloging the trade secrets, if the organization has only a handful of trade secrets to manage, then it is possible to use a company-developed management system to identify and track security measures. If, however, the organization's trade secrets are growing, there are software systems available that help ensure the company is managing its trade secrets in an efficient and effective manner. Finally, you should make sure the scope of the audit is appropriate given your company's resources, what you plan to do with the results, and what the company (and its shareholders) risk tolerance is when it comes to trade secrets and protection of company IP.

2. Communicate with key stakeholders and custodians of key information.

It is important to communicate the details of the plan to those members of the organization that have data relevant to the audit, such as human resources, legal, IT, engineering, and business representatives most knowledgeable on the nature of the trade secret. This phase is important from an educational standpoint as it demonstrates to your team members the importance the company places on protecting your trade secrets and proprietary information. Cross-collaboration across the organization will be essential in this step to ensure you have a solid understanding as to where the company's trade secrets are housed, who has access to them, and how you are (or should be) protecting them. Meetings with key stakeholders should focus on having the individuals identify what they consider the company's trade secrets/or confidential information to be. Have the members of the group explain how the information is protected. The members should also be asked about their knowledge of any breaches of trade secrets and confidential information and whether they believe additional security precautions should be implemented to protect the information. Another suggested step here to maintain the attorney-client privilege and protect from disclosure of the audit findings is to identify an audit lead or leads to liaise with in-house or outside counsel. The potential hazard of in-house counsel being the liaison is that a court might find the function being performed by the in-

house lawyer to be more business-related than legal with no attorney-client privilege protections afforded. For this reason, consideration should be given to including outside counsel in the audit to add an extra layer of protection against waiver of the privilege, as well as adding someone outside the company to provide input/analysis of the audit and its findings.

3. Gather relevant information.

During this step, the audit team should gather details through interviews of key people as well as collection of policies and procedures in place regarding the company's potential trade secrets, as well as any information regarding protection mechanisms in place. It is also important to tour the company's facilities, including R&D locations, test sites, and training and demonstration labs. Additionally, the company's intranet and website should be reviewed to determine whether the content includes potential trade secrets and whether access is limited.

4. Identify trade secrets

Identification of trade secrets is critical for several reasons. First, a company can't protect what it doesn't know it has. That may seem like an obvious proposition, but if a company is large or siloed, it may very well be that one segment of the business possesses trade secrets, about which the rest of the organization is unaware. If that is the case, it may be that there aren't sufficient security measures in place. Second, employees need to understand what information the company views as a trade secret so that they do not disclose such information outside the organization. Third, trade secret identification is essential to successfully defending a trade secret in litigation. If a company has not adequately identified and described the trade secret in a trade secret theft case, the claim could be dismissed. Most courts require specificity of the trade secrets involved early on in the litigation. By cataloguing and describing your trade secrets during the audit, your company avoids having to do that before filing the lawsuit, or in the midst of the lawsuit when time is of the essence. One way in-house counsel can help drive this principle is to work with your internal teams to develop an information security policy detailing how employees should access, treat, store, transmit, and — most importantly — protect company information.

What constitutes a trade secret will vary from company to company depending on the company's size, rate of growth, type of ownership, competitive situation, and type of business. Information that confers a competitive advantage may potentially be found in any part of the company's business and may include patentable inventions, manufacturing processes, data compilations, marketing and sales plans, financial information; business expansion plans, employee salary, and bonus structures; and identities of suppliers or subcontractors. It may also include technical information as the object and source of software that a company sells or uses; the program logic, file structure, and algorithms used in such software development tools, drawings, and product sketches; information storage devices, including tapes and discs or films; photographs; technical information and know-how related to unannounced company products; and strategic information concerning the company's products. Also included may be financial information such as sales data, cost and pricing information, pre-announcement quarterly financial results, profit and loss information, customer purchase or royalty information, and marketing information, including customer and prospects lists; mailing lists for company announcements; product acquisition candidates; product plans; planned release dates for new products; strategic relationships with other companies; marketing and product positioning strategies; dealer lists; or dealer and distributor sales reports.

The following questions can be used to help gain a better understanding of the nature of your company's trade secrets.

- What gives the company a competitive advantage?
- What information would competitors like to gain?
- What is it about the information that confers a competitive advantage?
- How long is the information likely to remain secret? For example, is it the Coca-Cola formula that may be kept secret for decades in a safe, or is it something a competitor is likely to discover or figure out in six months?
- What would competitors have to do to develop the same information through fair means?
- What is the economic value of the information? (What did it cost to develop? What would it cost a competitor to develop? How much does the information contribute to the company's revenue? What might a competitor be willing to pay to license the information?)
- What would the cost be to the company if a competitor were to access this information? Would release of the information put the company in a significantly disadvantaged position potentially impacting revenue and ongoing business opportunities?

5. Review policies, agreements, and security measures.

As noted above, it is a critical component of the audit to review all of the various trade secret related documents that govern or impact their protection. Not only will it allow you to catalogue and track those documents as part of your trade secret protection plan, but it also provides an opportunity to confirm all documentation is up to date and compliant with any new laws or regulations.

The information that should be gathered includes recruitment policies and procedures, employment policies and procedures related to protection and nondisclosure of confidential information/trade secrets, code of conduct, record retention policies, and network IT access and security policies. It is also important to review your employee agreements to make sure they are current and comply with any developments in the law. Be sure to review any employee agreements that include confidentially and nondisclosure obligations, return of materials, invention assignments, and restrictive covenants (noncompete, employee and customer non-solicit, forfeiture from competition, no hire, and nondisclosure).

As these policies and procedures are reviewed, consider the impact of any new laws, recent mergers/acquisitions, addition of any new business partners or business segments may require new agreements. Do the agreements contain the necessary components for your business? Hiring and exiting policies should also be reviewed to ensure incoming employees are instructed not to bring, use, or disclose confidential information from their previous employer, and outgoing employees are reminded of their obligations not to take, use, or disclose confidential information.

Limiting access rights

Companies need to ensure that permissions and access rights to confidential information are appropriately limited to provide access to highly confidential information only to those employees with a legitimate business reason to have access. Partner with your IT and/or security teams to understand who has access to what information and why. Companies should ensure employee passwords must be changed systematically on a regular basis to help avoid password theft and sharing among coworkers.

A particular focus during this review should be the nature and adequacy of the security measures in place. Access controls, roles and responsibilities, data management involvement, and system architecture should be reviewed, analyzed, and documented. This will help to determine any potential vulnerabilities.

Physical security, data security, legal reviews, third-party access, password encryption and protocols, and systems monitoring protocols should all be reviewed.

Some questions to consider during this phase include:

- Which employees have access to the information? Receptionist? Mail room clerk? Only top scientists?
- Can access to the information be further restricted without harming the company's business operations?
- Have the employees with access to the information all been instructed concerning the importance of preserving its secrecy?
- Is the information protected by computer passwords, confidentiality legends, and/or tiered levels of access?
- What other measures are used to protect the information?
- What other measures could be employed without adversely affecting the company's business operations?
- Is evidence of the company's independent discovery or lawful reverse engineering of its information preserved when documents are destroyed and email records deleted pursuant to the company's document retention policy?

Companies also need to take into account advances in technology as they evaluate their security measures. Involving IT personnel with knowledge of current technology (and accompanying risks) and computer forensics is essential. Risks worth mentioning here include:

- Employees using flash drives and personal email accounts to electronically transmit documents containing trade secrets.
- Employee use of personal devices, such as a cell phone, iPad, cameras, and portable music players to capture data.
- Employees leaking (deliberately or inadvertently) information using social networking sites and other internet forums.

With so many new developments in technology and applications, even the risk of inadvertent disclosure is on the rise. People commonly work on their smartphones, storing company data and information, and sharing information via social medial platforms. A company's failure to install extra levels of security for these types of risks may be used by courts as an indication of a company's failure to take reasonable measures to maintain secrecy.

6. Detect gaps in security

Once you have gathered and reviewed the information in step five, identify potential security holes. Some suggested steps include:

- Identify all organizations and individuals with access to the company's competitively valuable information and assess their needs for access.
- Identify past losses of competitively valuable information.

- Assess whether competitively valuable information is disclosed in sales presentations.
- Outside of California, North Dakota, and Oklahoma, where non-competes are unenforceable, are employees with access to valuable information asked to sign noncompete agreements that are enforceable under the laws of the state in which they are employed?
- Is everyone with access to competitively valuable information, including employees, prospective customers, customers or licensees; vendors and suppliers; and visitors, required to sign nondisclosure agreements?
- Is it possible for persons other than authorized employees to gain access to areas where such information is maintained or used, except with an escort and a badge identifying the visitor as an outsider?
- Could a competitor discover the company's trade secrets by examining documents the company throws out or things that the company sells for scrap?
- Are there other threats to the security of the company's secrets?
- Are hiring and employment practices sufficient to protect trade secrets and confidential information?
    - Are new employees asked during hiring process to determine whether they have knowledge of propriety information belonging to a former employer and, if so, whether that knowledge relates in any way to prospective job duties?
    - Are prospective employees screened to determine if they are subject to confidentiality and/or noncompete agreements with a former employer and, if so, when those obligations cease or whether they are enforceable?
    - Are new employees required to sign nondisclosure and invention assignment agreements?
    - Are new and exiting employees trained on confidentiality obligations and what the company deems confidential?
    - Are departing employees reminded of their confidentiality obligations?
    - Are departing employees asked who their new employer will be and what their new duties and responsibilities will be?
    - Is there follow-up to determine whether the departing employees were truthful concerning their job plans?
    - Are departing employees restricted access to trade secret information before their departure?
    - Are departed employees telephone and email records reviewed for evidence that the employees made preparations to compete before resigning?
    - Are laptops and desktop computers of departed employees collected immediately and examined for the presence of improper files or suspicious activity?

7. Report findings to key stakeholders with recommendations to fill security gaps

Depending on the outcome of your audit, you may have a very small list of action items or a list that seems almost too much to undertake. It is important that you think strategically about how you approach the findings with your specific audience. Companies have different cultures and different appetites for change. You want to make sure you have thought about both short term and long-term remedial actions that are aligned with your company's risk tolerance. If your remedial plan is not aligned with the company's risk profile, you are not going to achieve buy-in from the organization's leaders to dedicate time and resources toward the initiative. You may find there are some items that will be very easy to remedy, and others that might prove to be more costly and time-consuming for the company. Make sure you are seeking guidance from the stakeholders on what they view as the most pressing and precarious business risks while simultaneously providing practical guidance on the

legal risks associated with the outcome of the audit.

8. Implement a trade secret protection plan

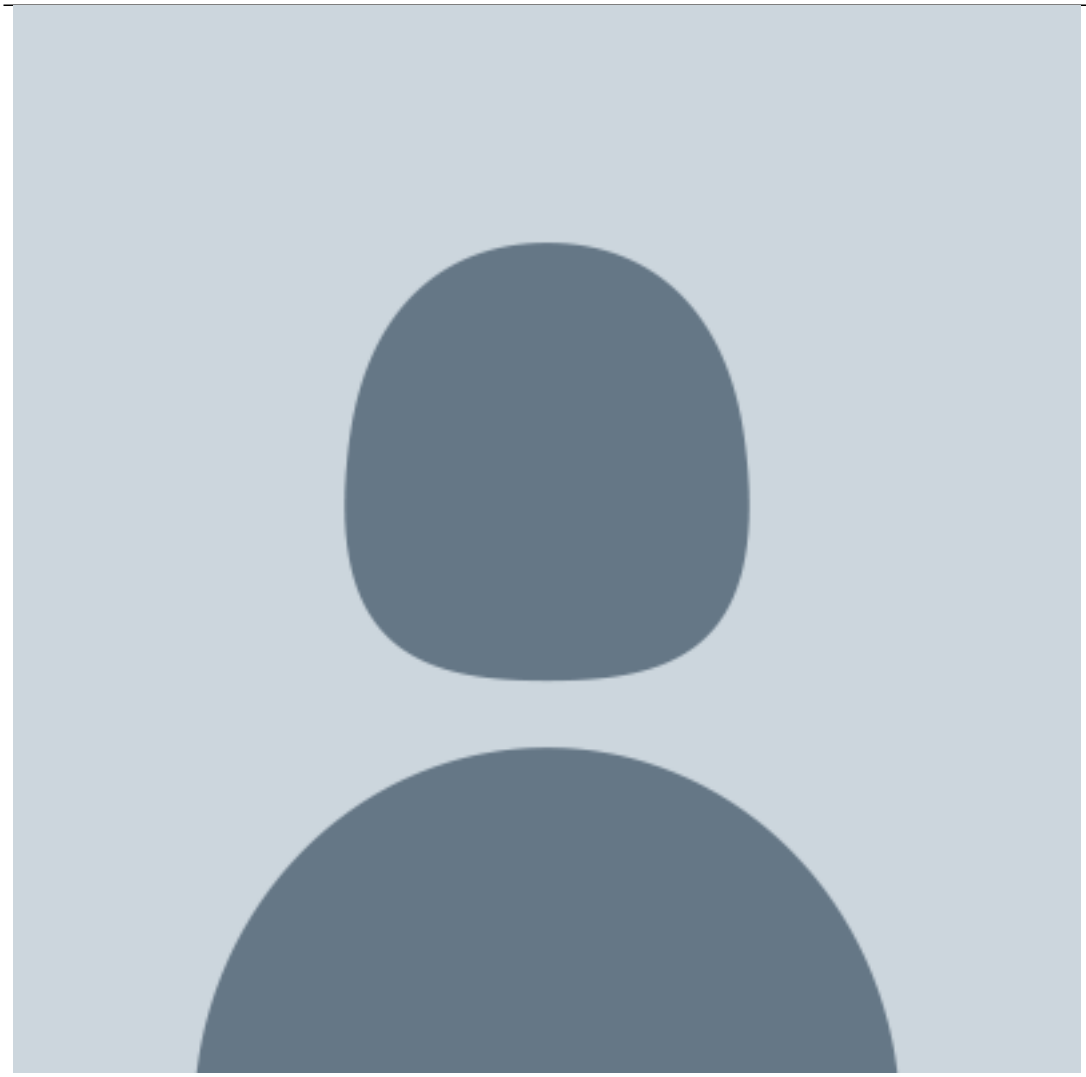
Once the company has had the benefit of the audit steps above, it should put a formal trade secret protection plan in place that can be followed on a consistent basis moving forward. An effective trade secret protection plan typically includes: (1) effective company procedures prohibiting the disclosure of company trade secrets; (2) a company individual or committee responsible for overseeing the trade secret protection plan; (3) a company workforce educated about the need to protect trade secrets; (4) maintaining confidentiality through training, agreements, and security; (5) effective employee intake and outtake procedures related to trade secrets/confidential information; and (6) periodic audits of trade secret protection policies and procedures.

Conclusion

Whether you are a multimillion-dollar corporation or a small startup, trade secret protection should be a fundamental element in your strategic business initiatives. The eight-step process laid out in this article provides a usable format for your company's trade secret audit. While some of the suggested steps may sound expensive and time-consuming, the reality is that the cost to an organization of disclosure and/or use of its trade secrets by competitors could be downright incapacitating. Again, collaborating with the business on audit objectives is critical to determining the scope of the audit and avoiding misalignment on cost and time management justifications. As you approach this topic, keep in mind this statement made by one commentator: "Just as mindfulness is rightfully understood as being key to a centered life, trade secret audits are essential to the continued success of the business."[1]

1 Trade Secret Audits - Why Bother?, David Cohen, David Cohen, PC, November 2017, KidonIPCorp, Kidonip.com.

Nicole Nguyen



Senior Director, Employment Counsel

NetScout Systems, Inc.

Katherine Perrelli

Partner and the National Litigation Department Chair

Seyfarth Shaw LLP