“Trade Secrets, it’s all about the Conversations”

By Dave Stevens, IP Attorney and Business Advisor, Stevens Law Group

“To keep your secret is wisdom; to expect others to keep it is folly.” William Samuel Johnson.”

KEY TAKE-AWAYS

1) Trade Secrets require unique and proactive care by their owners.
2) Continuing education is necessary for all employees to understand what the company considers Trade Secrets and how employees need to protect them.
3) Companies need to establish clear written policies, rules and regulations for protecting Trade Secrets and other company IP.
4) Companies need to have contracts between the company and its employees, contractors, vendors, customers and any person having access to their Trade Secrets.
5) Reasonable contract terms are preferred for nondisclosure agreements in employee and other contracts, rather than nebulous overly broad language that goes beyond actual Trade Secrets.
6) Collaborative arrangements between a company and third parties need to be clear on what each side considers Trade Secrets and how each person with access is expected to protect them.
7) Processes for sharing Trade Secret information between a company and potential M&A or license partner needs to be clearly defined and limited to information necessary to complete a transaction to minimize exposure to each other’s sensitive information and risk of misappropriation.
8) Trade Secrets need to be described in writing with detail and recorded with verifiable time stamps soon after they are conceived.

Sustaining Cultures of Innovation

In knowledge-based industries, cultures of innovation fuel companies' drive to innovate and lead markets. Within these company cultures, ideas among inventors and innovators are shared in protected environments. The introduction of sensitive information into these spaces needs to be kept secret from competitors until the company decides whether and how to protect them. The origin of these secrets is usually within conversations among employees who are tasked with a problem to solve, a product feature to create, or a goal to achieve. Once shared within the collective intelligence of a group, these secrets take on a new life and can transform a company’s technologies and products. These secret ideas are also considered trade secret assets that belong to the company, intellectual properties that have their own definition and unique laws that protect them.

Trade secrets are a unique type of intellectual property (IP). Unlike the intellectual property assets, including patents, trademarks and copyrights, there is no formal government established registration. And, once they are carelessly uttered in an unprotected conversation, protection can be weakened. Also unlike other types of IP, the existence of trade secrets and the mechanisms for protecting and preserving them depend solely on the deliberate actions of the owner. There is no type of government certification to secure secrets. But like all forms of intellectual property, no one will protect your secrets for you. As an owner of IP, you must take affirmative action to protect them before they are conceived, or you will lay yourself and your company a victim of theft. And, while bystanders may sympathize with victims of such theft, inadequate protection can justify the open use of stolen secrets. And, thieves can benefit from your unprotected trade secret information with impunity.

Companies adopting a wholistic IP strategy understand that the various types of IP are useful and valuable to the company. Each can be used as different tools that the company can utilize and rely upon as leverage in a company's business negotiations and activities. IP in its various forms provides a company with a valuable foundation of legal rights to have on hand as bargaining chips and visible deterrents to potential infringers of these rights. It follows that IP protection requires clear and rational policies guiding those with authorized access to sustain a culture of innovation.

Moreover, a company is wise to establish detailed business practice instructions for employees to follow to protect a company's trade secrets before information is created. This way, trade secrets can be secured in the normal course of business with fewer concerns over the risk of their potential loss. The secrets may even be transformed into other IP, including patent or copyright assets. But all of these types of assets are first conceived as secret information, and care must be taken to protect this information from the moment it is conceived to protect and sustain company value.

Once conceived, the unique secret is almost always shared in various conversations. At first, it is typically shared with some authorized people such as fellow employees, possibly contractors or customers. Preferably, all of the people involved in these conversations are authorized and under obligations of confidentiality with the company. But unless precautions are taken before the first conversations, there may be risks of unauthorized disclosure. These threats can potentially jeopardize the company's exclusive rights to the secret information. Adequate protection depends on precautions taken before the conversations, and these precautions need to extend to anywhere the conversations lead.

It's all about the Conversations

Hiring employees should be a celebrated event. Inviting new minds with new ideas and perspectives into a workplace gives new life to the work experience. Within a trusted culture of innovation, open conversations are the birthplace of great ideas. The more diverse, honest and unstifled human exchanges an organization experiences in open conversations, the more ideas can come to life and add value to an organization. And, the work experience becomes a hotbed of innovation resulting in inventions and ideas.

The best ideas and inventions can percolate to be shared, vetted, restated, consumed, and infused into products and services. All exchanges are supercharged by constantly nurturing the open conversation. The conversations often begin safely inside the company. But as a company grows, ideas and inventions are constantly threatened with disclosure in normal business operations and must be protected.

There is a big investment in these conversations, and shareholders among other stakeholders want security in their investments. All stakeholders have an interest in the proper care and nurturing of employees and preserving the sanctity of and trust in their conversations. The new ideas become innovations that create and improve the products and services sold by the company. Shareholders expect that all new innovations resulting from the open sharing of ideas within the workplace belong to the company. In personal relationships, people share ideas under an imagined umbrella of trust, and personal consequences result when trusts are breached. In the commercial world though, conversations are more complicated. The consequences can be expensive, and there are expectations of protections in promises and that give rise to rights in intellectual property. These promises must be well defined and carefully documented so that everyone can rely on the ownership of intellectual property. This way, people acting on behalf of companies can safely conduct business and shareholders can realize profits from their protected innovations.

All of this assumes that the company has policies and procedures for protecting their intellectual property. A company can file patents on the design, functions and operations of their product or service. The company can also retain copyrights as work-for-hire from employees contractors and vendors. It can also retain trade secrets through procedures of business conduct among internal and external stakeholders during certain engagements.

Before these conversations can begin however, proper care and nurturing of the company trade secrets must be cemented into a company's business practices.

Care and Nurturing of Trade Secrets

Trade secrets are a singularly unique intellectual property by the nature of their legally recognized protections. There is no federal registry of trade secrets, and there are no government entities that examine and certify secrets. Rather, trade secrets are established by the care and management of commercial secrets from the moment they are created by people who have obligations to assign them to the company. Part of this management is in contract, part is in company policy, part is in activity to identify and capture secrets and part is continuing education of employees' obligations to play their part in protecting a company's trade secrets. Flaws in any of these may jeopardize a company's ownership rights in its trade secrets and any other IP that results from a company's operations. Thus, care, nurturing and proper operational hygiene of a company's IP practices are essential to maintaining a company's trade secrets.

Contracts

Allocation of risk is central to all commercial contracts. Companies must strive to minimize its risk in all contracts, including NDAs of all forms. In companies where employees are not expected to have access to or create intellectual property, protections may not be necessary. Low tech companies such as retail shops or fast food may not depend on secrets to sustain their business. But, if your company depends on a secret information such as recipes, know-how, secret technology or customer contact lists for example, people with access to sensitive information need to be secured. It is wise to have contracts in place that make all business relationships clear and minimize the risk of trade secret losses. Obligations of maintaining secrets and assignment of related IP can be clearly set out in contracts so there is no confusion over any person's duties to protect and maintain any person's access to a company's sensitive information. For companies in knowledge-based industries, such contracts are essential.

Human resource (HR) professionals have well established resources to protect a company's trade secrets in contract. Employment agreements can take the first steps to define an employee's obligation to assign all rights to innovations created during employment with the company. Clear ownership in any patents, copyrights, trademarks and trade secrets can be subject to these agreements. Employees also agree when signing them that they will participate in any actions required to perfect the company's rights in these intellectual properties, including assignments and declarations required by government entities.

One common agreement used to secure a company's rights in ideas and innovations is a non-disclosure agreement or NDA. The company's first line of defense of their trade secrets is paved with them. These start with the employee NDAs signed at the beginning of employment with the company. For new employees, this might be their first NDA they have ever signed. Over time and subsequent employment experiences, other NDAs are signed and overlapping obligations occur. With these in place, employers are content sharing any information an employee needs to perform their job.

But this contentment might build a false sense of security. It may not be safe to assume that all employees are aware of what the confidential information is and how they are supposed to protecting it. Do employees even know what information is confidential? Are they aware of the obligations of the people to which they are disclosing the information? What do these agreements tell about the information and corresponding obligations to the people signing them? The answer varies widely.

Moreover, courts tend to read these NDAs closely often deem them unenforceable when they sweep too broadly. And boiler plate language that tries to parse out valid language in the presence of overbroad language may not save you, since the scope of the confidential information goes to the heart of the agreement. Unless limited by a clear and valid non-compete clause, an individual should be free to hire into another job and use their learned skills and accumulated knowledge. In California, non-compete clauses are unenforceable unless

you prove an employee actually stole company trade secrets, a difficult charge to prove. In New York, it is enough to prove that an employee had access to valuable trade secrets, but courts are reluctant to broadly deem particular company information a trade secret. And as a practical matter, it is not possible to customize NDA language for each of hundreds or even thousands of employees whose job definitions and responsibilities often change over time.

Making matters worse, different NDA scopes are often used by companies in many contracts both internal and external to the company. Most are different compositions of word salads that can range from being comically broad to uselessly narrow depending on which side you are on. In extreme cases, “Confidential Information” often “includes but is not limited to” a multitude of information categories and topics ranging from simply “ideas” to “know-how” to “business models” and other general information that may not even be protectable. These NDA components, sometimes referred to as “rotors”, are often repurposed, modified and shoehorned into many different company agreements without any tracking or monitoring safeguards. This usually extends ubiquitously into other agreements with all types of stakeholders beyond employees including temporary or permanent contractors, customer representatives, vendors, visitors of all types, and many other people who have different levels and types of access to company information. Promises are made and obligations are taken on by people who may not consider or even understand their responsibilities under the contract or the consequences of a breach. Even when a company tries to standardize NDAs or other agreement components, it often fails to realize how these play-out in practical everyday business practices of the company. What few realize is that a lack of clarity can cause unintentional misappropriation of trade secrets that might not even amount to a theft. If a person is not clear what information is confidential, let alone how they are expected to protect it, how can they even understand their obligations? Moreover, how can they ever be held culpable if any theft? The unintended result is that the company’s trade secrets are easier to steal, and efforts to try to enforce any company rights, real or imagined, are often futile.

Thus, a better approach is for companies to utilize reasonable contract language in their NDAs of all types. Efforts are better spent on taking greater care in defining and protecting their trade secrets. Companies are better served by addressing the actual risk of potential trade secret misappropriation. This approach would likely prove more effective in securing sensitive information rather than placing bets on nebulous or overbroad contract language.

Clarity in Commercial NDAs

It is not only a company's workforce that needs clear communication about a company’s trade secrets, but communication with outside entities that require access to a company’s trade secrets is equally important. Businesses often need to entrust sensitive information to contractors, partners, vendors and other entities to conduct business, such as for example to enable design and manufacture of products. Also, customers often are given early access to details of unreleased products, sometimes before they are even developed. In these relationships, careful communication is essential with clear commercial NDAs. And while the definition of what the company defines as confidential trade secret information may seem clear, issues often crop up over how these outsiders are supposed to treat this information.

One of the more common provisions of a commercial NDA requires the party that receives the secret information simply to protect the company's confidentiality in the same way that it protects its own sensitive information. Or, it may set out terms and include “but in any event the Recipient will treat Confidential Information at least as well as it treats its own confidential information”. But often the disclosing company has no idea what the outsider’s information protection program is, or how diligently it is executed by their representatives. So rather than relying on this lazy “boilerplate” language and trusting their program, it would be more effective to state specifically what protections you expect them to use when handling your trade secrets, and further include a reliable audit mechanism to ensure compliance.

Relationships become even more complicated when there is a collaboration agreement or joint venture, where two organizations have agreed to use their collective resources to develop a product or service. The separate parties to such collaborations are not naïve, they are hoping to gain an advantage with the resources of another company that they themselves lack. Both parties need to protect the valuable intellectual property that they each create, and this includes before, during and after the collaboration occurs. The company needs to be extra careful over assumptions that are made around the division of responsibility and also about ownership and control of innovations. The terms of the relationship are critical to defining who owns resulting intellectual property from the collaboration. It is also critical to understand that these relationships are by their nature temporary, so the terms of the arrangement must include the expected conduct throughout the relationship, from the beginning to the end. Thus, the inevitable conclusion of the arrangement must be negotiated at the same time as the collaboration itself. Therefore, all terms should be discussed in advance of beginning work.

And, the state of intellectual property each owns before the arrangement and intends to contribute needs to be clearly defined. If no new intellectual property is expected, as is rarely the case, then the contract can be simple, where the company retains all intellectual property it had before the arrangement. Depending on the contribution levels of each side, if it can be ascertained ahead of time, a company should carefully consider whether close collaboration is in fact beneficial to them. If the contribution level is perceived as lopsided against the company, then the terms should be strongly negotiated in favor of the company's ownership of any resulting intellectual property. This way the company can have control over how to protect it, giving a limited license to the other collaborating company. Both collaborating companies need to lay out the intellectual property they own before the collaboration, including trade secrets and other registered intellectual property, and thoughtfully lay out the licensing terms granted to each other if any after the collaboration. For any intellectual property assets created during the collaboration, each side needs to agree how to assign them. For property created exclusively by one side, the assignments can be exclusive to the creator.

For property created by joint inventors from each side, then there needs to be a clear decision on how to own and share it. These can be the most contentious terms of the negotiation, as each side wants to own as much resulting intellectual property assets as it can. Joint ownership seems like a fair result, but it is fraught with problems. For example, for the life of the asset, each side will have a say over how it is protected. One side may want to file patent applications domestically in the U.S. and possibly around the world, and the other side may or may not agree and simply want to keep trade secrets. These decisions can come with a very high price if worldwide protection is desired by one side. They can cost almost nothing if they are maintained as a trade secret, but risk of loss will always be an issue. And, during the life of the asset, if it is a patent asset, the many decision points along the life of the asset can be argued among each company's lawyers, further raising the cost of asset maintenance.

In one example of a recent joint development arrangement, two companies collaborated in a joint development and agreed to jointly own the assets. Upon completion of the collaboration, the patent attorneys of one side started arguing with the patent attorneys of the other side over how to respond to specific filings with domestic and foreign patent filings. The resulting legal bills were almost twice that of historical bills to the collaborating companies, and the goals of these assets were never made clear. The foreign filings began to grow exponentially in cost, with both sides erring on the side of extensive protection. Without clear contractual instructions, neither side had an easy solution to the growing problem. And, neither side had much leverage in the renegotiation of the contract after the collaboration was completed. The negotiated end result was that one side owned and prosecuted the patent assets, and the other side had a non-exclusive license, and both agreed on which countries to file and maintain the assets. This curtailed the rising costs and obviated the disputes, but it cost both sides a great deal compared to handling this problem before the collaboration.

Intellectual property policies can also dictate procedural steps to take before an employee or other company representative enters into a business relationship with a vendor. In the first instance, the employee has contractual obligations defining their employment with the company and to what extent the employee is authorized to use and share secret information. Specific practice instructions can be established to assess the

company's IP position with respect to the vendor before any trade secrets are shared. This way, an employee can be informed of what exactly is secret information and how they should handle it when conducting business on behalf of the company. This can be particularly valuable if you are paying a vendor to create or build something according to the company's technical specifications. Next, policies can require that a contractor or vendor agree to confidentiality obligations before they are allowed to engage with a company representative. Both parties, company and vendor or contractor, would be expected to bring past experience and knowhow to the table for initial discussions, and each has an interest preserving its own trade secrets and their employees' ability to continue use of their accumulated knowledge and skill in other engagements.

Consider for example a company laying out a blueprint for a vendor to build a software system for managing customer information. Not only can the customer information be a valuable trade secret, but processes for collecting and maintaining customer knowledge could be valuable to others in an industry. Thus, the company would have an interest in exclusive ownership of the system that manages their customer information. If the way in which the company collects, maintains and analyzes their customer data in a unique way, and if that way of managing the data gives the company a competitive advantage, it may want to own it exclusively from their competitors. Often, software vendor companies try to retain ownership of their data management tools so they can repurpose and resell them to other vendor companies - and this may include a company's competitors. In such a circumstance, the company can protect their IP before handing the blueprint over to the vendor. The vendor can be granted a license to build the system for the company, yet be restricted from repurposing or reselling the system to the company's competitors or others. In any case, the company is best served by assessing and protecting their own IP before any engagement with a vendor, so that there are no unexpected surprises after the engagement has concluded.

Mitigating Risks in M&A Due Diligence and Licensing

Two of the most common sources of trade secret risks are in potential acquisitions and certain licensing transactions. These and other transactions involve the company and an outside entity sharing potential sensitive trade secret information. Each side can justify requiring access to sensitive information because they need to know what they are paying for. Such transactions can be problematic if not carefully thought through with a protective strategy in mind. In these types of transactions, both sides have a legitimate need to share information in confidence, but an equally legitimate concern over risks in disclosing trade secret information.

For the acquisition target or potential licensor, there is the risk that the suitor will get an advantageous close look at their technology and possibly misappropriate it or use the information against them. The disclosing party worries of the risk of the other side receiving their valuable secrets, and then walking away in favor of another target or an internal project. Or worse, the investigating party could see otherwise secret technical information to determine if they infringe their patents. This often occurs, and if evidence of infringement is found, the negotiations can be terminated, and patent infringement lawsuits might be asserted against the target company. In some instances, the target company is eventually acquired by the bad actor for a discount after they are beaten down by the legal process. This can be an extremely costly risk that is worth considering before any such engagement.

And, on the other side, there is always concern that looking too closely at these external opportunities exposes the company to potential accusations of trade secret theft or misuse. If not careful, exposure to the target's trade secret information can contaminate their engineers with unwanted information. This can make it difficult for them to prove that their subsequent research was in fact their own. The target company could plant unexpected risk in the investigating company, making it difficult to defend from accusations of trade secret misappropriation or theft when product features are released or disclosed in filed patents or other published documents.

The level of risk on both sides varies with the intensity of the due diligence each side takes. Some may be required to inform the transaction, some may not. This is where both sides need to take care and not give up too much sensitive information and also take in only the secret information that is necessary for the transaction.

And this is where robust and thoughtful communication can be useful to both sides. It is to the advantage of both participants to discuss these risks openly before they engage in the disclosures. They can work together to devise ways to reduce the risk. For example, they could limit the timing or frequency of the disclosure to small steps, revisiting the need for information as they go. If either side decides to end the discussions at any point, then the two sides can more easily part ways without reduced risks of conflict or litigation exposure.

Thus, keeping open lines of communication along the way can help both sides work out ways to limit risk. Each side making clear the need and concerns around certain information will help minimize any risk of unnecessary disclosure of sensitive information. Even in intimate personal relationships, it is risky to assume that one side knows what the other is thinking. In business relationships, it is equally important to keep lines of communication open and robust to avoid misunderstandings and reducing risks of disclosure that may lead to conflict.

Company Policy

Company policies around ownership and maintenance of trade secrets and other IP can be established and published where anyone accessing their IP can see and be made aware of them. These include policy statements and instructions in company documents, websites, marketing and sales material and other places. This way, policies and intentions are made clear anywhere employees, contractors, vendors and other people are have access to sensitive information and participate in business operations. And it it not necessary for one policy to fit all circumstances, policies can vary with the level of sensitivity of particular information. Without a coherent policy, risk of conflicts in different business operations and company contracts increases.

Company policies around intellectual property should be focused on a wholistic IP strategy. The strategy should layout the purpose and reason around the treatment of different types of intellectual property by the company. Typically, this is set out by top level management, and all levels of upper management should be in agreement so that all stakeholders' management interests are considered and accounted for. It should serve as general guidance, a type of constitution that's sets high level guidance for rules and procedures to be established by middle management and administrators. It is essentially defining the soul of the company in how it treats its secret information. And it is a statement by the company intentionally recognizing intellectual property as a strategic asset for use in business operations and transactions.

A high level and less detailed policy can provide flexibility for middle management administrators in the day-to-day administration of the company's intellectual property and assets. If the company IP strategy ever changes, then the policy should be amended to reflect those changes, informing management and administrators with useful guidance to modify their procedures accordingly. It can also account for bottom-up input from middle-management and administrators to propose policy changes based on practical management and administrative experience for consideration by upper management. In smaller companies, it is simply guidance for all management and administrators.

Company Proactive Activity

Further to the administrative rules and regulations around the treatment of intellectual property, all company activity around intellectual property needs to be vigilant and proactive. In knowledge based companies, intellectual property in all of its forms is constantly created in the normal course of business. A company needs to have a proactive attitude toward identifying and protecting these assets while they are created, and to limit access to this information only to those who need it to perform their jobs. Thus, proactive activity and established practices in management and administration need to occur ahead of time before anything is created. Open awareness by all employees is necessary, and it needs to be encouraged and rewarded. From the creators of the intellectual property to management and business administration built around them, everyone needs to be vigilant and proactive in identifying and protecting intellectual property. This begins with the protection of novel ideas and information at their conception as trade secrets - and it requires thoughtful

consideration before ideas and information are created. This should be evident in all documentation, websites, product packaging, and anywhere company information is accessed or otherwise utilized.

It is also helpful to have open and notorious activity around IP protection. This includes locked doors with key card or biometric access, receptionists and even security at company lobbies to limit access to areas where company information is held. Having electronic sign-in sheets requiring all visitors to agree to confidentiality terms is also very useful in putting outsiders on notice when they come to visit. It also can include proper NDA language to contractually bind visitors to confidentiality terms that are advantageous to the company in case there is ever a breach.

This serves to remind insiders and put outsiders on notice that the company is serious about protecting its valuable information. It helps to have constant reminders that secret information is being vigilantly watched and protected. This way, if there is ever a breach of confidential information, the company will have strong evidence of activities and procedures for protecting their secret information.

Documenting Secret Information

Most importantly, the company must have a deliberate and clear process to document company trade secrets, reasonable efforts to protect its sensitive trade secrets, including monitoring and tracking who has access to their secret information. This is particularly true in the current business climate, where many more people are working remotely and communicating via video conferences. When information is shared to a broad audience, care must be taken in sharing trade secret information regardless of the size of the audience. All accesses to the trade secret information must be monitored and secured with passwords, and deliberate steps must be taken to secure the trade secret information through non-disclosure contracts and the like. Even an email requesting that certain information be treated as confidential is enough to show reasonable efforts to protect the information. Ultimate Timing v. Simms, 715 F.Supp.3d 1195 (W.D. Wash. 2020). In Amgen v. California Correctional, 47 Cal.App.5th 716 (2020), however, the court held that merely putting the word “confidential” on an email blast to 170 people wasn’t enough. Such a broad releasing of information to a large group would require stronger safeguards. And in a recent case involving video conferences, the contents of a video conference-based meeting among franchise owners lost confidentiality protection because the organizers did not require passwords or keep accurate track of who gained access to the call. Smash Franchise v. Kanda, 2020 Del.Ch. LEXIS 263. Thus, even if inconvenient, appropriate safeguards must be put in place for each and every person given access to the secret information.

Documenting trade secrets by a company is essential to proving possession and ownership of the information. The Defense of trade secrets Act (DTSA) defines an owner as one who has rightful possession of a secret. So mere possession is enough to establish standing to sue on trade secret misappropriation, and a company needs to secure ownership and not just hide the information. In Advanced Fluid v. Huber, 958 F.3d 168 (3d Cir. 2020), it was held that even though the plaintiff had developed the information under a “work for hire” contract that gave title to a third party, he had standing to sue. Thus, if a company ever needs to go after someone for misappropriating a trade secret, they must prove that they in fact had possession of the trade secret before it was misappropriated. This means that the information that the company considers a valuable trade secret needs to be documented, stored in a protected location and time-stamped in a manner that is verifiable. This should include the names of the creators of the information, the contractual obligation they are under (employee, vendor, contractor, etc.), details of the secret information, and a verifiable timestamp on the information.

Storing and timestamping sensitive information can be done in many ways, some more effective than others, and should include multiple and even redundant steps. It can be done simply by sending and internal email to someone in the company such as an IP administrator. This was clarified in a recent ruling this past year, Ultimate Timing v. Simms, 715 F.Supp.3d 1195 (W.D. Wash. 2020), where the court found that an email request to treat information as confidential was sufficient.

Trade secret protection can also include more formal processes such as filing of provisional patent application, where not converting to a non-provisional application will keep the information secret and also provide a verifiable government timestamped receipt of deposit. Other methods include storage in database internally with automated timestamps, automatic versioning storage for software, recording with a law firm, source code repository, software escrow, and other similar methods with safeguards. Once set up, a system for documenting trade secret information can be very low cost and convenient for any stakeholder who needs to access it.

With vigilant and proactive attention and activity around protecting company trade secrets, risk of loss is greatly diminished. And once company employees are educated and trained on the system, it begins to practically runs itself.

Company Education and Training

Ongoing education is essential to maintaining strong and valuable intellectual property culture for a company. The company must clearly communicate to its employees what exactly trade secrets are and how to protect them for successful business outcomes. While it is important for employees to know which particular information the company considers its trade secrets, it is also important to understand what types of information they should be on the lookout for to protect. The education can take on different forms, including published rules and processes, online tutorials, in-person training and lectures, and interactive workshops that give employees hands-on practice through activities and role playing. Setting up a type of IP university for the company can ensure collective involvement by all stakeholders and administrators and of course the creators of intellectual property for the company. Recreational exercises, games, hacking events, and even competition can be very useful in supporting collective involvement in a company's IP program.

Companies can establish a type of IP university with a well thought out curriculum. Employees can be educated early in their careers and take leadership positions to serve the effort. It is imperative that a company provide continuing education for new hires as well as refresher courses for all employees. Long term employees can benefit with reminders of what is secret to prevent them from forgetting or wrongly thinking that something is no longer secret once products release or services have gone on for some time. Trade secrets can possibly last indefinitely if cared for properly.

The company can establish certifications for continued education, and require certain courses be completed before employees are granted access to certain secret information. Licensed professionals such as lawyers and financial staff can possibly earn continuing education credit for attending and leading courses. A company can even invite outside technical people, customers, professionals or even competitors to attend their courses as a recruiting tool or a thought leadership or community leadership initiative.

In Closing

Trade secrets are a very unique intellectual property that requires proper care and nurturing to protect. At a minimum, trade secrets need to be recorded by the company with verifiable time stamps to ensure evidence of ownership at the time secret information is conceived. Proactive companies are best served by establishing clear and unequivocal policies, rules and procedures that are communicated to all employees and others who have any level of access to a company's trade secrets. So long as the company stays ahead of these conversations, it will minimize risk of loss and maintain optimum protection.