

Risk Mitigation and Due Diligence: Intellectual Property

“There are only two categories of companies affected by trade secret theft: Those that know they’ve been compromised—and those that don’t know it yet.”¹

--Attorney General Eric Holder

In 2015, a group of Chinese men incorporated a company, covertly on behalf of a Chinese manufacturer in Houston. Their aim was to steal trade secrets from a company that created foam material with commercial and military applications. They did so by offering high paying roles to employees of the foam manufacturer, a global engineering firm with a Houston subsidiary. Two employees from the Houston subsidiary eventually joined the new company and divulged the manufacturing processes to the Chinese corporation. Luckily the original manufacturers caught wind of the operation and notified law enforcement. Seven people were charged with attempted IP theft and were put on trial, facing 10 years in prison and severe financial penalties.²

Timely and accurate Information is a powerful weapon and influence which company succeed or fail in the market today. Because of this, highly sensitive or propriety information is usually tightly guarded in various forms of trade secrets and patents requiring Non-Disclosure Agreements (NDSs) before they are accessed. As such, hiring employees for highly sensitive positions that involve research and development, intellectual property, patents, in particularly innovative sectors like Life Science, Pharmaceutical and Technology demand a high level of due diligence to mitigate the risk associated with disclosure.

Vetting candidates for sensitive roles may involve an exchange of possible proprietary information, a firm must be diligent and thorough in not just hiring the right candidates but throughout the search process. Candidates often interview for positions at similar companies, and since they become privy to certain company details during the interview process, it could prove detrimental to a firm if passed along to their competitors. As such, firms seek to protect their most closely held secrets by requiring the interviewee sign an NDA before divulging their IP information.

¹ (Quinn Emanuel Trial Lawyers, n.d.)

² (Fields, 2017)

Currently, the process of interviewing for key leadership roles is as follows: candidates are identified, and those meeting the highest qualifications are interviewed in order to gauge their potential fit for the firm. The candidates who best fit are “short-listed” to a second round of interviewing often with an NDA signed by the candidate. The candidate pool is further curated into a final list of 2 or 3 candidates. When offers are likely to be made is when background checks triggered. Sometimes the background checks are done after the offer has been made, in which case it becomes a formality at best, and a disaster at worst.

Just because an employee is not in a senior role does not necessarily mean the role is any less critical. If administrative staff prepare or handle sensitive documents, the risk of insider threat is just as prevalent. In the federal government, administrative staff often carry the same security clearance that federal agents and members of the Intelligence community. Any contact, decisions or intelligence analysis is communicated in some form of a document. The entire eco-system of sensitive information must be bullet proof to discourage, minimize and guard against an external or insider threat

We advise clients to establish a Risk Management Profiles as part of the selection, hiring, and retention of the employees by implementing the following: Pre-Due Diligence; Screening Applicants; Target Specific Areas for Screening; and Continuous Screening of Employees. An employee’s Risk Profile will evolve based on a change in financial behavior, an arrest, drug and alcohol abuse, litigation, disciplinary action and pursuit of new employment.

- **Pre-Due Diligence**

Pre-Due Diligence is rarely followed but highly recommended, and the steps are as follows: shortlist a number of candidates; conduct background investigations to whittle down to candidates of a desired integrity; approach cleared candidates with an NDA and progress on with recruiting discourse freely. Clarity and informed discussion are key to making the right decision in any situation, but it becomes paramount when selecting for a senior or critical position. Screening short-listed candidates makes them more viable for the role, informs the interviewing committee of the candidates’ context, and removes one element of surprise from a vetting process that is often filled with (unpleasant) surprises. Once the Pre-Due Diligence of early background check is complete, information can be more free-flowing and disclosed as necessary. Permitting more sensitive discussions to take place. It also takes out some of the ambiguities and imperfect knowledge usually encountered in interviewing.

Background Investigations:

- Screening Applicants

Screening is scalable. When searching for a new General Manager, the screening process may be less intensive, using a different set of parameters when scouting a new COO or hiring a receptionist. Two main aspects should be taken into consideration; firstly, the influence a role has on the company as a whole and, secondly, the sensitivity of information the candidate will be made acquainted with during interviewing.

Screening should be performed prior to an initial interview as it would allow the recruiting party to quickly reduce their shortlist, thus saving time and effort further along the process. Yet again, screening should be relative to the role, as such, the categories of search can be tinkered with after considering the importance of a role.

- Target Specific Areas for Screening

Screening is a major administrative cost and deciding how much muscle goes into the process is integral to the efficiency of recruiting. The first step must be to create a foundation of specific search categories considered important.

STOP HERE 1/28/19

A few areas that may be focused on at a base level are civil complaints for patent infringement, previous violations of NDAs, previous legal troubles, and what regulatory changes they enacted in their previous firms. These factors will be helpful in guiding and informing a firm about their candidates.

- Continuous Screening

One area of screening that is often neglected but important is Continuous Screening. A master practitioner of CS is the United States government. Positions requiring access to highly sensitive information or security clearances involve periodic background investigations. However, the government also routinely updates these checks by monitoring employees' circumstances and life events.³ These recurring checks, while routine, will have specific, evolving points of inquiry which will reflect the employee's evolving levels of accountability and responsibility. As employees progress through their career and become privy to more classified information, their background too should be more closely

³ (Clark, 2017)

scrutinized. However, lower level employees with little access to important information are not be as regularly screened.

CS can be considered the gold standard in terms of securing clearance for individuals with access to highly sensitive information. This is for a very good reason. Over the course of their lives people's events and circumstances change, as well as their surroundings. As an example: an exceptional employee joins a firm but three years later is in the midst of an ugly divorce and is in financial trouble, according to CS. They are not exhibiting any signs of distress, but should they be allowed access to sensitive information that determines company strategy? At issue is the trustworthiness of an employee at any given time, but also her ability to make difficult decisions under stressful circumstances. In other situations when an employee will need access to certain confidential data beyond the scope of current responsibilities, the company needs to make an assessment if additional screening is required and implement a standard policy that applies to everyone. But conceptually, senior management must make a change of a Risk Profile as part of their Risk Management. Finally, transparency about CS can keep good employees above board, the way a routine drug testing can keep airline employees clear. Perhaps a way to aptly decide on how much the trust placed onto this employee could be found by doing Continuous Screenings every 12-24 months on them.

This may seem overkill, perhaps even draconian, At the same time, it is crucial to accept that people and their circumstances change, and along with those changes, sometimes behaviors and decisions. Now in keeping with that notion, one must never assume an employee is a stanchion of integrity – no matter their seniority or apparent loyalty--90% of trade secret prosecutions saw the defendant labelled as “insiders” who had garnered the trust of the senior management.⁴

Best Practices to Protecting Intellectual Property

In addition to using background checks to monitor a change in Risk Profiles and keep a firm's intellectual property safe during the interviewing, hiring, process, and while the employee is working with the company, there are steps that can be taken to prevent ex-employees from divesting information to competitors. Such as, using physical barriers like crypto digitizing the information to prevent unauthorized people from accidentally viewing the information. Instead of printing out documents and leaving it for anyone to view it, it may be wiser to keep sensitive information digitized as to prevent non-required readers from becoming aware of such information. A very simple yet effective method is simply labelling

⁴ (Quinn Emanuel Trial Lawyers, n.d.)

documents and reports as 'Confidential'. Once that label has been stamped upon some document employees are instantly made aware of the potential consequences they face for violating the confidentiality of information.

Trust is arguably the highest value that anyone can offer anyone, whether the recipient is a person or an organization. Simply put, the best practice to safeguarding intellectual property comes from doing background checks early before hiring and regularly after hiring, being transparent about what information is being checked and what must stay confidential, and above all, doing due diligence, rather than blindly trusting.

Works Cited

- Clark, C. S. (2017, July 10). *Government Warms to Continuous Monitoring of Personnel With Clearances*. Retrieved from Defense One: <https://www.defenseone.com/technology/2017/07/government-warms-continuous-monitoring-personnel-clearances/139314/>
- Fields, A. (2017, September 29). *DOJ Alleges Seven Defendants Conspired To Misappropriate Trade Secrets*. Retrieved from Orrick: <https://blogs.orrick.com/trade-secrets-watch/2017/09/29/accounts-frozen-doj-alleges-seven-defendants-conspired-to-misappropriate-trade-secrets/>
- Quinn Emanuel Trial Lawyers. (n.d.). *Federal Prosecution of Trade Secret Theft*. Retrieved July 6, 2018

i mask intelligence™