Introduction

Many companies have a serious gap when it comes to protecting their assets: trade secrets. With data breaches grabbing headlines, and companies historically relying on the comparatively traditional protections of the patent laws, trade secrets are often neglected. Because protecting trade secrets requires effort and input *across departments*—from intellectual property counsel to human resources, from information technology officers to compliance counsel—it sometimes falls between the cracks, with no one functional group or leader owning the issue. But, with trade secret theft on the rise, and verdicts in some theft cases having neared a billion dollars, trade secrets must become a priority.

In particular, companies must be aware of and avoid three common shortcomings relating to trade secrets. *First*, many companies laser-focus on threats from outside the company (e.g., hackers, data breaches), ignoring the real and significant threat from within – their employees or contractors. *Second*, feeling safe in the belief that their data will not be appealing to bad actors, companies fail to take "reasonable measures" to protect their trade secrets, rendering them unable to assert a legal claim when theft occurs. *Third*, while some companies have started to focus on data *leaving* the company, many ignore the flipside of the coin: the growing and costly risks inherent in new employees *bringing* trade secrets from their former employers. Below is a discussion of and practical guidance for avoiding these three common pitfalls.

Issue 1: Ignoring the Threat from Within

Companies cannot focus solely on the risks from *external* breaches or hacks: theft or misappropriation by employees or contractors is pervasive. A recent study by Symantec found that a staggering 50 percent of employees keep confidential company data when they leave the company, with more than 40 percent revealing that they planned to use company data at a new job and 44 percent indicating that they did not believe it to be a crime to use a competitor's trade secrets. Pause on that information for a moment. There is likely no other context in which nearly half of the at-risk population believes that conduct is not a crime, while prosecutors and investigators are stacking up conviction after conviction for that very conduct. Given this mindset, it is not surprising that one analysis published by *BNA's Patent, Trademark & Copyright Journal* found that more than 90 percent of the prosecutions from 1996 to 2012 under the Economic Espionage Act involved corporate "insiders" rather than external thieves.

Theft by insiders also is comparatively easy to pull off—no sophisticated means or criminal masterminds required. With portable storage drives, cloud storage, and personal email accounts, employees have multitudes of easily accessible means to copy or forward valuable company data in an instant. And, the cost for an employee to execute this theft is cheap, as a flash drive that looks like a pen or a credit card can cost just a few dollars. Theft of volumes of data can thus be both quick and easy, and—without affirmative mechanisms in place—difficult to detect.

The interconnected nature of the internet also provides even the average non-tech-savvy employee with many tools to quickly transfer data. For example, in a case recently filed in California, a former employee at Zynga used the cloud-storage provider Dropbox to upload 760 files about future products, pricing models, and employee compensation, allegedly to pilfer this information to benefit a competitor. According to a lawsuit filed in federal court in Texas, a former employee of Zenimax took another approach by copying emails before leaving for rival Oculus VR. In example after example, employees—with little effort and without using sophisticated methods—are able to steal valuable data and quickly transfer it outside the company.

The threat is exacerbated as employees increasingly job-hop. Long gone are the days where an employee

works his entire life for one company and retires with a golden watch. Instead, the interconnected global marketplace continues to create an environment for increased employee mobility. The Bureau of Labor Statistics confirms this trend, as the average employee tenure dropped to 4.2 years in 2016 from 4.6 years in 2014. A LinkedIn study published in April 2016 showed that millennials job-hop more than any previous generation. With the global market dynamics and a workforce infused with untethered millennials, the threat of trade secret misappropriation from internal breaches has never been greater.

The takeaway is clear: in this easy-access, high-mobility landscape, companies need to take a hard look in the mirror and implement policies and protocols focused on theft from *within*. Basic protective measures should include limiting access to valuable trade secrets (i.e., not allowing every person with a logon ID to access every document). Additional security measures, beyond just passwords and building keycards, should be considered, such as preventing employees from mounting USB devices or blocking personal email accounts. Thoughtful and robust "Bring Your Own Device" and remote access policies should also be employed. And, when an employee leaves the company, steps should be taken immediately to shut off the employee's access, to collect all devices, and potentially to monitor for suspicious activity, such as large downloads or emails to certain domain names. Companies that do not take such measures should be prepared to find valuable data having walked out the door—potentially to a competitor.

Issue 2: Believing Data Protection Is Not Necessary

While not every company will be a high-priority target for bad actors, **all** companies need to take active steps to protect the information that differentiates their business. Every company has information worthy of protection—that which would be valuable in the hands of a competitor, whether it be manufacturing specifications, formulas, pricing lists, data from failed R&D, or customer lists. In fact, according to CREATE.org, intangible assets like trade secrets and other intellectual property make up an estimated 75 percent of U.S. Fortune 500 companies' value. What companies often learn after it is too late is that failing to invest to protect their secret sauce can cause that information to lose its protection as a "trade secret" under state or federal law. Thus, when theft occurs, they are left without a remedy.

The key to obtaining legal protection is to take "reasonable measures"—a requirement under both the federal Defend Trade Secrets Act and most state trade secret statutes. The law does not require companies to take extreme measures or employ every possible protection. However, failing to take any steps, or comprehensive enough steps given the nature of the business or high-value of the trade secret—a surprisingly too-common occurrence, particularly for growing companies—will lead a victim-company to find itself kicked out of court without a remedy. For example, a federal court in New York recently dismissed a case brought by a secondary ticket market software company because, while it required employees to sign a non-disclosure agreement and identified some confidential information in the employee handbook, the marketing and sales teams included trade secret information in client interactions without having the clients sign a confidentiality agreement. Despite obvious theft, the court dismissed the trade secret misappropriation claim, given the lax protections. Other courts have denied trade secret misappropriation claims when the company has taken little or no steps to protect what the company views as valuable information.

A company should not find false comfort in the fact that it does not have data it thinks would lure hackers or internal bad actors. Failing to take steps to prevent external data breaches or theft based on such a belief could undermine an argument the company took "reasonable measures," thereby undermining the company's ability to obtain legal remedies when theft—either from internal or external sources—occurs. Indeed, companies cannot approach data protection in a disjointed fashion—separately considering protections against outside data breaches and internal trade secret theft. Instead, companies must consider data protection holistically to ensure that that they can enjoy the protections of the trade secret laws.

Issue 3: Failing to Prevent the Importation of a Competitor's Trade Secrets by a New Employee

An important piece of the trade secret puzzle that companies too often ignore is data *entering* the company. The flip side of the insider theft problem discussed above is that employees take the stolen data to their new jobs. As the new employer is likely the deep pocket—rather than the employee-thief—the new employer faces the risk of long (and potentially extremely costly) litigation. In fact, according to a 2017 Stout Advisory report, the average length of a trade secret litigation from 1990 to 2015 was four years, and the plaintiffs won a staggering 69 percent of the time at trial, with a lower percentage of such cases being dismissed than other types of complex civil litigation. Couple that win-rate with the types of damage awards being seen across the country — many individual damages awards exceed 100 million dollars – and you can understand why these cases are becoming the litigation *de jour* for plaintiffs' firms.

The risks stemming from a trade secret suit are particularly high given that the DTSA provides certain advantages to the plaintiffs. First, some courts have rejected the argument that the DTSA creates a heightened pleading standard that would require a trade secret misappropriation claim to be pleaded with "reasonable particularity." Therefore, in some jurisdictions, a plaintiff merely needs to allege a fairly boilerplate theory that the information taken relates to any form or type of trade secret, defined by the DTSA as "financial, business, scientific, technical, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, process, procedures, programs or codes." This large scope of information that could qualify as a trade secret aids a plaintiff's ability to bring a suit, and reduces a defendant's ability to dismiss a suit in the early litigation stages. Second, some courts have concluded that a plaintiff can bring a suit even if the defendant has not *used* the trade secret based on a theory of "inevitable disclosure" of the trade secret. This means a plaintiff's suit can proceed if the defendant's new employment will inevitably lead him to rely on the plaintiff's trade secrets.

An entire article could be written about the number of high-profile, and highly expensive, "new employer" trade secret cases that have been litigated in recent years. To avoid this type of litigation—and the associated costs, disruption, and potential reputational damage—companies must take steps during the interviewing and onboarding processes to prevent a competitor's trade secrets from entering the company, or, at a minimum, provide the company with a solid legal defense if ever accused of conspiracy to misappropriate trade secrets. For example, a company should review a new employee's agreements with his former employer; should inform the employee during interviews and onboarding that the company wants no information from the employee's former employer; should ask the employee to certify that he has not brought and will not use any trade secrets; and should consider, if the risk is high, alerting the former employer, or even monitoring for large uploads during the employee's first weeks of employment.

Conclusion

Companies can open themselves up to significant and costly risk by having tunnel-vision when it comes to their approach to trade secrets. It is a multi-faceted issue with internal and external risks, including risks stemming from data entering and leaving the company; yet many companies are not taking a holistic enough approach—incorporating insights from and involving HR, IT, and legal—to safeguard the trade secrets that are valuable to the company's success.

The time is ripe for companies to address these issues and include trade secrets as part of their risk register, because not only is the threat of theft real and potentially devastating, but recent changes to U.S. and

European laws increasingly have empowered companies to protect their trade secrets. For example, the passage of the Defend Trade Secrets Act in 2016 has armed companies with a federal remedy (including even an *ex parte* seize power) if theft occurs and the European Union has passed major legislation to increase trade secret protection, Council Directive 2016/943, 2016 O.J. (L 157) 1 (EU). Meanwhile, recent Supreme Court cases have narrowed the scope of patentable subject matter, the mechanism often used to protect assets in the past. Thus, having a robust approach to trade secrets as part of a company's legal arsenal is increasingly valuable—and, with the growing mobility of the workforce and the ease at which data can be taken, increasingly necessary.

Steven Grimes is a former federal prosecutor, an experienced trial lawyer, and a former Chief Compliance Officer and senior litigation counsel for a global publicly-traded Fortune 500 company. Steve's practice focuses on compliance and data security counseling, sensitive internal investigations, government interactions, and complex litigation.

Shannon Murphy is a member of the firm's Global Privacy and Data Security Task Force, focuses her practice on internal investigations, data protection counseling, and complex litigation, particularly matters involving potential criminal liability or trade secret issues.