The Goldilocks And Three Bears Dilemma: Adopting Reasonable Measures To Protect Trade Secrets In The New Work Environment

By Steven R. Kursh and Pratike Patel

Abstract

The COVID-19 outbreak accelerated the growth of work from home at many enterprises. An important factor enabling collaborative work from home was the use of video conferencing, shared development project work tools, and other technology-driven resources for virtual enterprises. Given that many employees are choosing to remain working remotely from the office on at least a part-time basis, software companies need to reassess and update their policies and practices regarding the protection of intellectual property, particularly trade secrets. The phrase commonly used in the law regarding trade secrets is "reasonable measures." While certainly under the umbrella of security practices to protect against hacking and malware, reasonable measures to protect trade secrets often involve different, albeit related objectives. There are numerous best practices and policies that warrant review and potentially adoption, but managers face the dilemma of choosing which policies and practices to adopt since such policies and practices can be costly and create unnecessary constraints for employees, customers, and other stakeholders. Obviously, no one wants their organization to devote the time, money, and other resources to working with legal counsel to litigate misappropriation of trade secrets. Prevention is the preferred alternative. Managers, however, need to decide, "how much is enough" regarding reasonable measures what we label the Goldilocks Dilemma. This paper provides a review of reasonable measures that can be considered and used by software companies when assessing and adopting measures to protect their intellectual property, particularly trade secrets.

I. Introduction

Now that COVID-19 has largely passed, it's time for software companies to take a step back to reassess their work environments and policies related to protecting their intellectual property (IP), particularly in regard to having "reasonable measures," the criteria used with trade secret litigation.

Most, if not all, software companies with staffs larger than a few people likely have some policies regarding their IP, for example, having Nondisclosure Agreements (NDAs) and provisions related to confidentiality in their agreements with third parties and employees. Larger software companies typically have a broad range of policies and measures in place reflecting their ability to make investments in security-related activities as well as other factors. Publicly traded companies that do business outside of the United States must also implement policies related to IP and technology risks with international operations.

No matter the size and scope of a software company the reality that many managers face is determining just how far to go with the adoption of policies and related reasonable measures to protect their intellectual property, particularly trade secrets. These reasonable measures may certainly fall under the umbrella of security policies to protect against hacking and malware, but reasonable measures often involve different, albeit related objectives. The management challenge is further compounded by the expectations of many team members to continue, at least partially if not nearly 100 percent of the time, working remotely using collaboration tools and other technologies.

The CISO (Chief Information Security Officer) or anyone tasked with developing and implementing polices to protect their organization's IP generally has to be selective in what she does; only a small percentage of companies have the resources to do nearly everything possible to protect their IP. Not enough protections could potentially result in loss of trade secrets and issues with potentially customer proprietary data becoming public. Too many protections can slow down product development, inhibit innovation, and cause frustration among key personnel, partners, and customers.

II. The Goldilocks and Three Bears Dilemma With Trade Secrets

This tradeoff between too much and too little with policies and practices regarding reasonable measures, like the porridge ("too hot, too cold, just right") in the fairy tale "Goldilocks and the Three Bears," is further compounded by resource constraints at many software companies.

While an independent observer may readily be able to find gaps in nearly every company's policies and procedures relative to his "ideal set of reasonable measures," the reality is that most software companies face multiple demands on monetary and time resources, and the essence of management is determining priorities for those resources. The key word is "reasonable,"

and "reasonable" depends on multiple factors that will vary significantly among organizations.

Management needs to decide the when/where/how to invest in policies and practices regarding their organization's intellectual property, particularly trade secrets. In our work, we frequently speak with managers and staff attorneys tasked with security-related issues, including development and implementation of reasonable measures at their companies in regard to trade secrets. We hear overwhelmingly laments that there just aren't sufficient resources, and that having security measures against even primary security risks like hacking and malware, let alone in the related activity of taking reasonable measures to protect trade secrets, is a daunting task requiring ongoing investments and vigilance. They recognize that having security measures in place to mitigate the risk of hackers and malware is critical (as evidenced by the recent event involving Colonial Pipeline, JBS Foods, Kaseya, a Florida-based IT company, and other organizations).

By contrast, having reasonable measures in place to protect trade secrets requires somewhat different objectives and accordingly, focus and types of efforts. From the perspective of software and, more broadly most technology companies, nothing is more important than intellectual property. In fact, some people label the software code and trade secrets of software companies as the "crown jewels." Indeed, the risks are great for not taking steps to protect your crown jewels.

Investing today can potentially result in your avoiding costs and problems in the future. Consider, for example, the effect of a competitor, domestic or foreign, who gains access to and exploits your confidential and proprietary information. Even worse, imagine that the competitor has already taken advantage in the marketplace of the knowledge gained, and your organization is not even aware of their actions. Or, that your organization learns of the misappropriation, but does not want to invest in litigation that may not be successful for, among other reasons, the defendant's argument that your organization did not take appropriate and reasonable steps to protect its intellectual property. You don't want to be in this position of having to make the phone call to your legal counsel and then devoting substantial time to working with your legal counsel with litigation to protect your company's IP.

Hence, the Goldilocks Dilemma: making the ongoing investment in reasonable measures to protect your trade secrets while ensuring that your company doesn't spend too much or holds back your team, all while providing access and making the use of your products/services by customers easier, not harder.

Our objective in this article is to provide some general guidance in responding to this dilemma. Our perspective, one based on many years of experience working at software companies, working at universities, conducting research, and working with companies and their legal counsel in litigation matters related to intellectual property, is that one single approach does not fit all companies. Instead, we hope that what we recommend here provides guidelines for further discussion and consideration at your company.

We turn now to a discussion about why trade secrets are different than other types of IP. Here we emphasize that the adoption and ongoing investment in reasonable measures with trade secrets differs from the options companies have in regard to patents, copyrights, and trademarks. We also provide some background regarding software and trade secrets.

■ Steven R. Kursh, Ph.D., CSDP, CLP,
Founder,
Software Analysis Group,
Cambridge, MA 02142
E-mail: s.kursh@softwareanalysisgroup.com

■ Pratike Patel,
Senior Consultant,
Software Analysis Group,
Cambridge MA 02142
E-mail: pratike.patel@softwareanalysisgroup.com

The remainder of the paper provides a suggested set of reasonable measures for management at software companies, particularly SaaS companies, to consider implementing. As part of this section, we'll also discuss some of the parties involved, *i.e.*, employees, consultants, partners, customers, suppliers, service providers, and others, with an emphasis on how the reasonable measures undertaken should vary depending on each of these constituencies. Additionally, we'll cover the types of information your organization likely deals with on a continual basis and how the reasonable measures you undertake should reflect the fact that some of your intellectual property is particularly important to protect with more stringent reasonable measures.

Although our focus is on software companies, particularly SaaS companies, the discussion that follows is applicable to most technology-driven organizations.

We note, furthermore, the importance of working closely with your legal counsel to establish appropriate measures to protect your trade secrets. Our work focuses on the technical and business steps you may want to consider. Ultimately, though, you will be working with counsel to decide the what, when, where, why and how to take reasonable measures.

III. Types of Intellectual Property

First things first—let's distinguish trade secrets from other types of intellectual property. Many of us are likely familiar with patents, copyrights, and perhaps, even trademarks. Trade secrets? Well, we may know trade secrets are one type of intellectual property and

some of us might reference the formula for Coca-Cola as a trade secret, but what exactly qualifies as a trade secret with software companies? We'll discuss what qualifies as a trade secret shortly. For now, let's briefly discuss the other types of IP and note differences with copyrights, trademarks, and patents as compared with trade secrets.

With copyrights, the U.S. Copyright Office and other agencies note that copyrights are a form of expression and that the 1976 Copyright Act generally gives the owner of the copyright the exclusive right to reproduce the copyrighted work, to prepare derivative works, and other rights. It's generally known that a software company cannot, with exceptions involving open source, government software, and with permission of the owner, use the software code from another company or individual.

A copyright owner must enforce the copyright without the aid of the copyright office. In our experience copyright analysis involves comparing and analyzing the two sets of code in what we and others label a "side-by-side comparison." This process is complicated when one company develops its code drawing from the original set of code but is written in a different programming language. A related issue is also, of course, access—how did the company that drew on the original set of code get access to it? By contrast, the analysis of trade secret misappropriation does not always require comparing the source code from the parties, a topic we discuss below.

With trademarks, the USPTO notes that a trademark or service mark is different than copyrights and patents. A trademark is a word, name, symbol, or device used in trade to reference the source of the goods as well as to distinguish those goods from goods offered by others.

A service mark identifies and distinguishes the source of the service as compared to other sources. An owner of a trademark or service mark must enforce the trademark or service mark without the assistance of the USPTO.

Trademarks and service marks provide the rights to stop others from using a confusingly similar mark. Neither trademarks nor service marks prevent others from making or selling the same respective goods and services. In effect trademarks and service marks relate more to marketing/sales (as well as strategy) versus the development and provision of software products. This is a critical difference among several between trade secrets and trademarks/service marks.

Turning to patents, many of us are likely familiar with patents from our work as well as general news stories related to patent disputes. Patents are quite different than trade secrets. Per the USPTO, a patent for an invention is the grant of exclusivity by the U.S. Government, typically for a term of 20 years from the date when the application was filed. Patents provide the right to exclude others from making, using, offering for sale, or selling the inventions in a patent. There are three types of patents: utility, design, and plant. For most software-related inventions, the patent would be a utility patent. The owner of a patent must enforce the patent directly; the USPTO does not get involved directly with enforcement.

There are many critical differences between trade secrets and other types of IP. Unlike with other types of IP, there is no application process for trade secrets with the USPTO or any government agency. There's no prosecution period like with patents, no formal filing of a portion of the trade secret unlike with copyrights, and no registration like with trademarks and service marks. Nor do trade secrets expire like patents. Companies have clear and consistent avenues to protect against misappropriation of patents and copyrights. There is generally no need to protect *a priori* patents and copyrights with the exception of the source code if the copyright or patent includes source code. Yet, even with this level of protection, the task is much easier than much of what companies consider to be technology and business trade secrets.

There are many other differences as well and, in regard to your organization, it is important to speak with legal counsel to determine the best form of IP protection.

IV. Turning to Trade Secrets

So, what exactly is a trade secret? Here are some guidelines that incorporate technical-related factors:

First, a trade secret must meet legal standards. Until 2016 those standards were established by state laws. In 2016, President Obama signed the Defend Trade Secrets Act (DTSA). Although the state trade secret laws are still applicable, our discussion here will focus on the DTSA.

Per the DTSA a trade secret is defined as:

"…all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

(A) The owner thereof has taken reasonable measures to keep such information secret; and

(B) The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person

who can obtain economic value from the disclosure or use of the information."

Importantly, the DTSA prohibits "misappropriation" of trade secret information by "improper means."

Misappropriation per the DTSA is defined as:

(A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

(B) disclosure or use of a trade secret of another without express or implied consent by a person who—

(i) used improper means to acquire knowledge of the trade secret;

(ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was—

(I) derived from or through a person who had used improper means to acquire the trade secret;

(II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or

(iii) before a material change of the position of the person, knew or had reason to know that—

(I) the trade secret was a trade secret; and

(II) knowledge of the trade secret had been acquired by accident or mistake.

Improper means:

(A) includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means; and

(B) does not include reverse engineering, independent derivation, or any other lawful means of acquisition.

As noted above from a literal reading of the DTSA language, a trade secret may consist of any information if the owner of the trade secret has taken reasonable measures under the circumstances to keep the information secret, and the information derives economic value from not being generally known to, and not being readily ascertainable through proper means by, others in competition with the trade secret holder.

Hence, customer lists, know-how, and importantly, user-facing software components, including features, functions, architecture, design, workflows, and processes, could constitute trade secrets. Additionally, a trade secret could consist of combinations of characteristics and components, even if some or all of those components are individually in the public domain.

The big BUT is that the company must take reasonable measures to protect its trade secrets. Like much of life, the devil is in the details, and we will shortly turn to a discussion of what could be "reasonable measures" at your company.

We know from our experience in the field working with companies that many organizations that fail to invest in technologies and policies to protect their IP often regret not investing on a timely basis, resulting in the proverbial "closing the door after the horse has left the barn."

Keep in mind, too, as noted above, that protection against hacking and malware is not a substitute for taking reasonable measures to protect trade secrets. Obviously, implementing security protections against hacking and malware is important for all organizations, businesses, government agencies, and not-for-profits. Nearly every day we hear about hacks and ransomware attacks against businesses, government agencies and not-for-profits. Often the perpetrators are working from locations outside of North America and in most incidents, are difficult to track.

Designing and implementing reasonable measures to protect trade secrets is somewhat different. Research has shown that the primary risks associated with trade secret misappropriation are associated with employees, past and present,[1] and business partners, including third-party companies and individuals on a contract basis. (An exception is software hacked by competitors.)

Since there is no standard for what constitutes "reasonable measures," management at some software companies believe that just implementing information security practices is sufficient to protect their trade secrets. There are many well-known standards for these practices such as NIST, CIS and ISO 27001. Unfortunately, the successful implementation of a security framework is not sufficient for protecting trade secrets because most are stolen by people and organizations that the vendor thought could be trusted.

V. Software Evolution and Implications to Trade Secrets

All of us are aware that software applications over the past 50 years have evolved from performing basic functions such as email, word processing, and web browsers to performing more complex business processes. Basic software applications, such as email and word processing, have features and functions that

1. David R. Hannah, "Keeping Trade Secrets Secret," *Sloan Management Review*, April 1, 2006.

competitors can easily understand and use without directly interacting with the application.

Complex applications that have robust business processes and logic built into their user interface and are integrated with other applications are usually a different story. Generally, companies offering complex applications, particularly SaaS, have additional risk because how they do "it," *i.e.*, "the secret sauce," can often be reverse engineered.

Cloud computing, furthermore, has created more complexity in protecting intellectual property, particularly trade secrets. Many observers were well aware nearly a decade ago that the cloud would enable and enhance connectivity among companies and others while creating increased risks for misappropriation. Additionally, the rapid pace of innovation among software companies has added further opportunities for misappropriation.

SaaS companies need to be particularly mindful because of the risks associated with bad actors, such as customers, third-party companies that have been provided access by customers, partners, and hackers, accessing their software.

VI. Reasonable Measures: Six Suggestions

As noted above, there is no one single or even set of actions you should take to ensure that you have sufficient reasonable measures in place to protect your trade secrets. Keeping in mind, too, the "Goldilocks rule" that the porridge should not be too cold or too hot, here are six general suggestions based on our experience:

First, and most important, you should consider implementing measures that go above and beyond normal business operations, including actions you take to prevent hacking and malware. Technologies and practices such as virus software, malware software, operating system security updates, firewalls, and secure passwords are typically considered among the minimum actions that organizations should take.

New cybersecurity techniques in the past several years have become mainstream quickly because of the publicity surrounding high-profile security breaches. Such techniques may be applicable at your company.

Employers' responsibilities for taking reasonable measures now extend to smart phones and tablets. Employees today rely on apps on these devices as much as a computer to perform their work regardless of where they are. Traditional desktop business applications such as Microsoft Office and Adobe Creative Cloud are on tablets and phones.

It is very common for employees to use purpose-built mobile apps such as Concur expense management software, Salesforce customer relationship management software, Slack, and Trello to perform their work. Most SaaS applications have a mobile app because it is one of the key features many companies evaluate when selecting a SaaS solution. Many companies also build apps for their own internal custom software applications.

With the increased use of mobile devices, including personal devices becoming more prevalent (BYOD), organizations have to take reasonable measures in protecting trade secrets on these types of devices similar to how they are expected with computers. Mobile device management (MDM) software allows enterprises to configure smart phones and tablets so that they are secure.

MDM has become sufficiently mainstream for some companies that iOS and Android have native support for it. Alternatively, techniques such as "sandboxing" applications can keep a company's data secure while recognizing the realities of today's BYOD movement.

A general rule of thumb is that if a technical measure is a feature in consumer cloud services, then you may want to consider adopting a similar practice. For example, GMAIL has two-factor authentication (2FA) so that their primary users, consumers, can have better protection over their account than what passwords alone offer.

A secondary benefit of 2FA is that it requires the use of something you have, *e.g.*, implementations that use retina scan or fingerprints, which cannot be shared, which makes it difficult for authorized users to share their account for dishonest reasons.

As noted above, a significant percentage of trade secret misappropriation happens with insiders—employees, whether present or previous, suppliers who have password-protected access to your systems, customers who have password-protected access to your systems, third-party contractors that have password-protected access to your systems, and others who acquire improper access to your systems. Assess the key risks and implement policies accordingly.

Second, it is critical to recognize that you are facing a moving target and must constantly reassess your reasonable measures and make improvements. Vigilance is key and throughout the process you should have a risk management perspective. Depending on the size of the company, the CISO or whomever is charged with implementing reasonable measures should have an information protection team, even if the "team" is just herself, which is often the situation at small companies, to monitor, reassess and respond to risks.

A risk management philosophy must be considered and applied to business ventures, suppliers and partners because they can become a future competitor who could misappropriate their knowledge of your

trade secrets to create competitive products and services. Access to new trade secrets and continued access to existing ones should be reviewed and rationalized on a continual basis with an eye on minimizing what is shared, because today's partner could be tomorrow's competitor.

Third, working with legal counsel, you should have a set of documents that provide a headstart when negotiating with prospective business partners, subscribers (*i.e.*, customers), reviewers, and others. This includes NDAs, subscription and/or license agreements, and other agreements that your counsel deems necessary. Be particularly aware of definitions of confidential information and the need to limit the length of time the confidential information from the disclosing party is available to the recipient.

These agreements should be reviewed and updated periodically depending on the advice from counsel. An article published by the World Intellectual Property Organization suggests creating agreements, policies, procedures, and records to establish and document protection.[2] All such documents should usually be created working with counsel.

Fourth, develop, implement, and update internally-driven procedures for employees, independent contractors, suppliers and others. This includes the following:

1. For employees, a set of processes from the time of hire until the employee leaves the company is helpful. This includes a NDA, employee training, employee handbook, periodic training, and exit interviews. The process should include, at a minimum, prohibitions of sharing emails and documents; encryption of drives; use of passwords with all teleconferencing calls; 2FA protection of all systems; embargo of storage media such as flash drives; exclusion of all company-related materials on desks; no use of personal devices; marking documents, reports, and other printed materials as confidential; tracking unusual access; and downloads of company information.

   Employee access to information should be on a need-to-know basis, *i.e.*, through role-based security, immediate cutoff from the company's systems once the employee has left, and robust off-boarding practices that include reminding ex-employees of their continued responsibilities regarding IP.

   It is also helpful for employees to learn and use good practices in regard to some confidential information being more important than other confidential information. Software professionals often consider source code sacred, not realizing that the flows of software applications are critical, particularly regarding business rules and logic. The experiences the company has gained, what we label "what not to do," is often as valuable as knowing what to do. Database architectures, customer lists, and product plans are similarly important. Customer data and information, including end-customer information with SaaS software, requires particular attention.

   Also, consider equipment that you give to employees for use at home. Such equipment should be managed in ways that are closely similar to what is done at the office. For example, at-home equipment should have access to up-to-date security patches, virus updates and security settings such as automatic screen saver with password protection due to inactivity.

   We suggest that you suggest to employees working from home not to use Google Home and Amazon Alexa in their at-home workspace. Same with social media.

   Employees needing to connect to the office should use VPN technologies whenever possible. We recommend that policies and practices be implemented to ensure WiFi connections from home are secure. Employees should generally not access company resources from public WiFi connections, such as those at Starbucks.

   Offboarding practices must also include collecting relevant equipment from ex-employees.

2. For contractors and suppliers, we suggest NDAs; periodic reminders, but no less frequently than once a year regarding the company's polices regarding trade secret protections; tracking activities on the company's systems; immediate cutoff from the employer's systems once the contractor or supplier is no longer formally engaged with the company; and periodic review of what access is required to fulfill their obligations.
3. For external sales personnel, distributors, and others involved in marketing consider having similar policies and practices as you have with employees, as well as additional training to remind them to keep live demonstrations limited in scope. In-person meeting practices such as having attendees sign an NDA need to continue in the virtual world.

Ensuring that meetings and presentations done virtually using video conferencing technologies, such as Zoom, require additional safeguards such as using meeting unique IDs, passwords, waiting rooms, and the disabling of recordings.

Fifth, develop, implement, and update externally

2. Pamela Passman, "Eight steps to secure trade secrets," *WIPO Magazine*, February, 2016.

driven procedures. Technical controls may be important because they involve the use of role-based access that ensures only the minimum information necessary is provided within a limited timeframe. These controls may need to be reviewed periodically and updated as necessary.

It is important that companies consider consolidating activities across all their systems to track website activity with products like Pendo or Segment. The tracking should not be just your SaaS site, but logs to your software and underlying code, as well as design information and other kinds of records that have activity-logging capabilities. Unusual user activity, such as multiple logins from the same account in disparate geographic locations, accessing a large number of files in a small period of time, and multiple failed attempts to access resources that the user does not have permissions to use may be red flags requiring investigation.

Sixth, don't waste precious time and resources trying to identify trade secrets *a priori*. We understand that some analysts recommend taking this step, but based on our experience, this measure may be applicable primarily with companies that have multiple divisions with trade secrets among multiple business areas, for example, formulas and in manufacturing processes. With software, however, this measure may not be appropriate. Those of us that work extensively with software applications and specifically code are well aware that much of the software itself cannot easily be broken into disparate and independent pieces. Think of a three-egg omelet with meat, veggies, and even some fruit like tomatoes. While one could separate out the meat, veggies, and tomato, it is essentially impossible to separate out each one of the eggs separately. Also, the eggs would be impacted by the other ingredients. ■

Available at Social Science Research Network (SSRN): *https://ssrn.com/abstract=4019548.*

VI. References

[1] David R. Hannah, "Keeping Trade Secrets Secret," *Sloan Management Review*, April 1, 2006. Available: *https://sloanreview.mit.edu/article/keeping-trade-secrets-secret/*.

[2] Quentin Hardy, "Cloud Computing is Forcing a Reconsideration of Intellectual Property," *New York Times,* October 11, 2014.

[3] International Organization for Standardization, "Isoiec Information Security." Available: *https://www.iso.org/isoiec-27001-information-security.html*.

[4] Pamela Passman, "Eight steps to secure trade secrets," *WIPO Magazine*, February, 2016. Available: *https://www.wipo.int/wipo_magazine/en/2016/01/article_0006.html*.

[5] U.S. Department of Commerce, National Institute of Standards and Technology, "CIS Security." Available: *https://www.cisecurity.org/controls*.

[6] U.S. Department of Commerce, National Institute of Standards and Technology, "Cyberframework." Available: *https://www.nist.gov/cyberframework*.

[7] U.S. Department of Commerce, National Institute of Standards and Technology, "Trade Secrets Protection in the US." Available: *https://www.nist.gov/system/files/documents/mep/marinaslides.pdf*.

[8] U.S. Patent and Trademark Office, "Patent Basics." Available: *https://www.uspto.gov/patents/basics*.

[9] U.S. Securities and Exchange Commission, Division of Corporate Finance, "Intellectual Property and Technology Risks Associated with International Business Operations," CF Disclosure Guidance: Topic No. 8, December 19, 2019. Available: *https://www.sec.gov/corpfin/risks-technology-intellectual-property-international-business-operations*.

[10] Josh Vevs, "Building On The Gains Made From Remote Work," *strategy+business*, *PwC*, July 7, 2021.