quinn emanuel trial lawyers
quinn emanuel urquhart & sullivan, llp

Legal Concerns Clients Are Having About Covid-19

"Reasonable Measures" To Protect Trade Secrets At Risk With Employees Working-From-Home Amid Covid-19 Crisis

April 2, 2020

Amy Candido
amycandido@quinnemanuel.com
Phone: +1 415-875-6309

1) Introduction

Millions of employees across the United States have abruptly transitioned to working-from-home, many for the first time, as a result of widespread efforts to stop the spread of the coronavirus.[1] Employers must be cognizant of the increased risks to their trade secrets associated with these remote employees and take steps to ensure that their valuable assets will be protected.

Legal protection of trade secrets depends on whether a business has taken "reasonable measures" to keep the information secret. Some of the situations that businesses now find themselves in create a risk that courts may find businesses have fallen short. For example, employees may take advantage of being subject to less supervision while working-from-home and use this time to access and take trade secrets for their own gain if businesses have not taken steps to limit and monitor access. Employees abruptly transitioned to working-from-home due to the current crisis are likely to be using their own personal devices and Wi-Fi networks. Employees' personal devices and home networks may lack appropriate password, virus and security protections, and may be shared with family members or housemates—posing increased risk to any remotely accessible trade secrets. The systems businesses use to allow their employees to work-from-home are also likely to be stretched during this crisis due to unprecedented demand. This may cause even well-meaning employees to engage in riskier workarounds simply to get their work done, such as using personal email, messaging or cloud platforms, downloading trade secrets to personal computers, cellphones or clouds, and printing trade secrets.

If the new risks precipitated by the Covid-19 crisis catch businesses off guard, they have the potential to destroy significant value invested in trade secret development. For example, in 2020, a jury

awarded Motorola Solutions $764 million for Hytera Communications' theft of trade secrets relating to mobile radios.[2] In 2018, a jury awarded HouseCanary over $700 million for Amrock's theft of trade secrets relating to its real estate valuation technology,[3] and ASML, a Dutch company, won $223 million against a U.S. competitor for theft of its trade secrets.[4] Many technology start-ups and businesses operating in technologies such as artificial intelligence protect their most valuable technologies with trade secrets, not patents, and the value of those technologies is immense.[5]

In this article, we address the legal framework for protecting trade secrets, key issues businesses face in protecting trade secrets during the Covid-19 pandemic, and some of the measures businesses can implement to mitigate the risks to their trade secrets posed by employees working-from-home. Those steps will reap immediate rewards today by minimizing the risk of theft or inadvertent disclosure and, if necessary, will help businesses enforce their trade secret rights in court in the future.

2) Businesses Must Use "Reasonable Measures" To Protect Their Trade Secrets

A trade secret owner's duty to be vigilant in protecting its secrets from disclosure is built into the very definition of a trade secret. For information to be legally protected as a trade secret, its owner must use "reasonable measures" under the circumstances to keep it secret. Both the Uniform Trade Secrets Act (UTSA) and the federal Defend Trade Secrets Act (DTSA) define a trade secret as any confidential information, such as financial, business, scientific, technical, economic or engineering information, which both:

> (1) derives independent economic value, actual or potential, from not being generally known to the public or other persons who can obtain economic value from its disclosure (*i.e.,* it provides a competitive advantage to a company or organization); and
>
> (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[6]

Thus, in order to pursue a claim for trade secret misappropriation, the owner must show that it used "reasonable measures" to protect its trade secrets.[7] Satisfying this requirement not only shows that the trade secret is in fact valuable to its owner, but it reduces the risk of inadvertent disclosure or theft in the first place.

Trade secret owners are not required to take every conceivable measure to maintain secrecy. Rather, courts assess what efforts are reasonable "under the circumstances" based on the nature and value of the trade secret information sought to be protected, the ease of theft, the extent of the threat of theft, and the particular field of knowledge or industry.[8] Courts also recognize that what efforts are reasonable may differ based on the size and resources of the business.[9] For example, at a small family-run business, personal trust may be easier to manage than at a Fortune 500 company.

The reasonableness inquiry is a typical risk analysis, in which threats to secrecy are measured against the costs of reducing the risk and the value of the information sought to be protected. What may be reasonable in one context may not be reasonable in another. As one court put it, "taking precautionary measures to protect secrets imposes both direct and indirect costs on the owner of the secret, and thus 'perfect security is not optimum security.'"[10] Security measures need not be "extreme and unduly expensive."[11] However, courts expect to see that a business has taken reasonable steps specifically designed to protect the disclosure of its trade secrets above and beyond "general protective measures."[12] Failure to take such steps is taken as "persuasive evidence that the secret has no real value" and is undeserving of the law's protection.[13]

Companies should seek to strike a balance between the information security processes that will provide effective protection and legal enforceability of their trade secrets and other business realities, including cost, operational efficiency and information sharing demands necessary to drive innovation and

support business operations. In the best of times, designing and implementing an effective and sustainable trade secret protection program is a challenging and multi-faceted endeavour driven by the unique considerations of each business. During an international pandemic, ensuring that your business is using "reasonable measures" under the circumstances to protect its trade secrets holds new and unprecedented challenges.[14]

3) Practical Advice for Businesses On "Reasonable Measures" To Protect Trade Secrets When Employees Work-From-Home

In light of the threat to trade secrets posed by an entire workforce working-from-home, prudent businesses should identify their key trade secret information and assess whether they are taking "reasonable measures" to protect that information. As always, what is reasonable during this crisis will depend on the specific facts, but there are certain steps cited by courts as "reasonable measures" that a prudent business should at least consider. Those measures most relevant to employees working-from-home during the Covid-19 pandemic are discussed below. Ultimately, what is reasonable for any given business to protect its trade secrets will most likely be a multi-pronged approach, combining those measures with the least cost and the greatest return.[15]

a) Identify Trade Secret Information For Employees

Employers should consider defining in clear and simple terms what information is considered a trade secret and what is expected of employees who have access to that information. Given the nature of the trade secrets at issue, it may be appropriate to identify trade secrets with specificity in some cases, while in others it is sufficient to focus on broad categories of data.

Courts emphasize the importance of advising employees of the existence of a trade secret as a "reasonable" measure to protect it.[16] For example, in *United States v. Tien Shiah*, the district court found Broadcom's security measures "barely satisfie[d] the standard of reasonableness," highlighting the fact that Broadcom's "overbroad" designations of information as confidential made it hard for employees to determine what information was actually confidential. The court stated that Broadcom should have made clear to its employees what information is a trade secret and how to handle that information.[17] Similarly, in *Yellowfin Yachts, Inc. v. Barker Boatworks, LLC*, the Eleventh Circuit found that Yellowfin's security efforts were unreasonable where Yellowfin expected its employees to know that its customer information was trade secret based solely on verbal statements of policy and verbal warnings.[18]

b) Limit Trade Secret Access To Those With A Need To Know

Employers should consider limiting access to trade secrets to only those persons, groups or departments with a "need to know."[19] This may be done with electronic trade secret information (as well as physical documents or prototypes), by restricting access to specific systems, databases, programs, or documents to only those with a "need to know."[20] The ideal, if feasible and consistent with the employer's cost-benefit analysis, is that each employee has access to only those trade secrets which they truly need in order to do their job. Indeed, one study of U.S. trade secret litigation found that a court is over ***18 times*** more likely to find that the trade secret owner engaged in "reasonable efforts" if it restricted access to certain persons, such as by adopting "need to know" rules.[21]

Notably, according to the FBI, providing access privileges to those who do not need them is a factor which increases the ease for thievery.[22] In addition, where access to the trade secrets is not restricted to those with a "need to know," courts weigh that fact against finding reasonable measures have been taken.[23] For example, in *Cumulus Radio Corp. v. Olson*, the district court found reasonable steps had not been shown, even though the plaintiff had nondisclosure agreements with its employees, because the alleged trade secret information "was readily accessible 'on a shared computer network' that 'could be reviewed by anyone who had access to the computer system.'"[24] In other words, Cumulus Radio's failure to limit access to employees with a "need to know" doomed its claims.

c) Use Passwords And Secure Logins To Access Corporate Networks

Part and parcel of limiting access to those with a "need to know" is requiring passwords and secure logins to access corporate networks. When it comes to electronic trade secrets, courts look for password protection as a necessary condition to finding that reasonable measures were taken.[25] Indeed, one court found that requiring passwords for employees to access their personal directories on the business's shared server was "not enough" because passwords are "normal business practices in any business." The court added: "An employer must use additional measures to protect the confidentiality of information he considers to be a trade secret."[26] Not surprisingly, using password protection to limit trade secret access to specific employees with a "need to know" is cited approvingly by courts as a reasonable measure.[27]

Employers also may find it useful to use passwords to restrict access to particular systems, or specific drives, files, folders or even documents.[28] Moreover, password-protection increasingly involves password strengthening requirements (length, upper and lower case, numerals, and non-alphanumeric characters), password renewal requirements (renewing on a regular basis and not repeating passwords), or multi-factor identification (something you are given plus something you know, or a password plus authentication via text or phone call).

d) Use Firewalls Or Other Security Software To Protect Your Network

Employers should consider using firewalls or other similar security software to protect their trade secrets by creating a barrier between their trusted internal network and untrusted external networks, such as the Internet and their employees' various home networks. Judging what is reasonable under the circumstances, courts may expect at least some firewall or other baseline of perimeter security from all employers, and more advanced security measures for larger, more sophisticated businesses and businesses subject to known cyber-threats. Courts may view perimeter security as akin to having a lock on your front door. Employers who place a high value on their electronic intellectual property should not short-change perimeter security and should be vigilant ensuring that their security technology remains up-to-date going forward.

Courts cite firewalls among the "reasonable measures" to protect trade secrets stored on a network.[29] For example, in *United States v. Tien Shiah*, the district court discussed Broadcom's network security measures:

> Furthermore, Broadcom protected its electronic data through its information technology team, which managed firewalls, fire transfer protocols, intrusion detection software, passwords to access the Intranet, a layer of protection between the Intranet and Internet, and selective storage of files.[30]

The district court found Broadcom's network security measures on the whole reasonable.[31]

Additional network security measures that employers may want to consider, depending on their circumstances, include data loss prevention software, network segregation, avoiding aggregating trade secrets in a single, centralized network location where a breach could be severely problematic, and stress testing designed to ensure that all systems and system security measures function properly in an environment where most or all employees are working-from-home simultaneously.

e) Consider Encryption For Any Particularly Valuable Information

Employers may want to consider encryption for any particularly high value trade secret information. Such information, for example, could include the "secret sauce" technical information in a highly competitive industry where, if the information got out, the business would be destroyed. Encryption may be used for particular files, computer discs, servers, email traffic and other items to restrict unauthorized access, both by unauthorized employees and third parties. Courts currently recognize encryption as

evidence of a trade secret owner's reasonable efforts to protect trade secrets, but have not yet reached a point where failing to use encryption is viewed as a failure to take reasonable measures.[32]

f) Require Employees Working-From-Home To Use Secure Technologies

Employers should consider holding employees to the same standards for protection of company information when working-from-home as when working from the office, and clearly communicate policies and procedures specific to working-from-home. Depending on each company's unique circumstances (such as their threat environment and the nature and value of the trade secrets at issue), employers may consider the following non-exhaustive list of practical measures to supplement a company's existing internal policies and procedures to address issues that may be raised by remote employees:

- Require certain minimum home security measures for employees' home Internet networks, including password protection for any Wi-Fi network and limitations on access to that network.[33] For additional security, consider requiring multi-factor authentication upon each login to a company portal and/or requiring employees to use a virtual private network (VPN) or other encrypted/protected means to access the company's system.

- Require a company-sanctioned level of anti-virus software, anti-malware software (with regular updates) to guard against cyber-attacks and other security lapses that could compromise confidentiality.

- Require that all devices used to remotely access the company network are password-protected with passwords changed at regular intervals, have hard drive encryption, and remote-wipe capabilities if lost.

- Require use of the employer's document management systems with document check-out and check-in.

- Restrict each employee's network access to only those network locations or segments that the employee needs to use, with appropriate security for those locations. This is an application of the "need to know" concept discussed above to the company's remote network. For additional security, consider imposing additional credentialing in order to download certain sensitive data or prohibit such downloads altogether. For example, consider prohibiting downloading data or specific data to employee's personal devices, cloud accounts and/or through personal email accounts.

- Use email filters to restrict communications from and to potentially risky or suspicious locations, to prevent transmission of particular files, and/or to guard against phishing or malware attempts that could pose a risk to trade secrets.

- Impose USB and other portable device restrictions, which may include prohibiting the use of such devices or the blocking of USB ports altogether, in order to protect trade secret theft, malware or device damage and unauthorized copying and downloading (even by employees with no bad intentions).

- Impose software app whitelisting or blacklisting to limit the potential risks from untested or unknown computer programs operating on the company's systems or interacting with the company's information. There is a risk that employees use publicly available apps with the intention of building efficiency, but failing to investigate or understand the privacy, ownership and protection of information shared through such apps.

As the remote workforce needs to rely on phone, email and instant messaging systems over in-person meetings and casual conversations in the office, additional opportunities for risk are created by the

sheer volume of electronic communications and the possibility that employees will communicate outside the company's secure systems. Employers can protect against some of these risks by ensuring that their email and messaging systems are and remain encrypted and secured, and by encouraging employees to use those secure systems for their work-related communications. However, as some employees will inevitably be tempted to communicate using text messaging on their personal devices and private chat applications, employers should consider their tolerance for those risks in formulating a policy regarding the use of such forms of communication for work purposes. In any event, employers should encourage employees to use good judgment about when, where and how they discuss work-related matters outside of the company's secure systems, if at all.

Finally, employers should remember that any policy is only as good as its implementation. If the security solutions are too cumbersome and unwieldy, employees will figure out their own work-arounds—usually at an increased risk to security. Accordingly, if employers include employees in the decision-making process and seek employee buy-in, new security solutions and policies will be more likely to succeed.

g) Consider Marking Trade Secrets

Employers may want to consider whether it is feasible to mark or otherwise label their trade secret information. For example, employers may explicitly put a legend, label, footer, digital watermark or electronic tag on trade secret documents or files. Similarly, employers may set up reminders that pop up every time a remote employee logs into the company's systems or into a particular database to act as a reminder about the need to keep such information secret.

The immediate practical benefit of marking is that it puts employees on notice that the information is a trade secret and must be handled according to the company's policies and procedures regarding trade secrets. In addition, courts have relied on the fact that trade secrets were marked confidential or secret to find that trade secret owners took "reasonable measures" to protect their trade secrets.[34] Marking may also help the victim of a trade secret theft establish that an unauthorized third-party recipient of the trade secret had "reason to know" that the information was not free to use.[35]

Absent marking, courts will consider other evidence that the alleged trade secret misappropriator had notice that the specific trade secrets were confidential or secret.[36] However, absent such notice, courts may cite the lack of any "confidential" or "secret" marking as a reason to find that the trade secret owner did not use "reasonable measures" to keep it secret.[37]

Moreover, if a company undertakes a program to mark its documents, but then fails to do so or does so inconsistently, that can be problematic. Inconsistent labeling may be cited by courts as undermining a company's secrecy efforts. For example, in *United States v. Tien Shiah*, the district court cited Broadcom's inconsistent labeling as one of the "deficiencies" in its information security measures:

> Broadcom was not clear about which documents should and should not be marked confidential. Shiah was directed to use a template for all PowerPoint presentations containing markings to indicate confidentiality, but there were inconsistencies about which other documents were marked confidential. Broadcom did not have a comprehensive system in place for designating which documents were and which documents were not confidential. A better system could have made it easier for employees to determine which documents were confidential.

In addition, the FBI has identified the lack of labeling or incorrect labeling of trade secrets as a factor which may increase thievery.[38]

h) Consider Corporate Policies And Procedures To Identify What Information Is Trade Secret And How It Should Be Handled

Clear corporate policies and procedures for maintaining the confidentiality of trade secrets which specifically address issues that arise when employees work-from-home have significant benefits. If employers do not have such a policy and one cannot be prepared quickly, employers may want to send an email or memo to employees setting out expectations and reminding employees of their obligations to protect trade secrets and any existing confidentiality policies.[39] While there is no one-size-fits-all set of policies and procedures that are right for all companies,[40] courts look for the existence of a written policy regarding the confidentiality of trade secrets as evidence of "reasonable measures."[41] Courts look for corporate policies and procedures that identify what information the company considers to be a trade secret and/or confidential and how such information should be handled by employees.[42]

Some case examples may be helpful. In *Freebird Commc'ns, Inc. Profit Sharing Plan v. Roberts*, Freebird's lack of any policies requiring that its allegedly trade secret customer information be kept confidential was detrimental to its claim. The district court granted summary judgment against Freebird, finding it did not use "reasonable measures" to maintain the information's secrecy: "Freebird did not have any policies regarding the protection of the alleged trade secrets, such as policies restricting the use of personal phones or computers for business, policies requiring that computers containing such information be password-protected, or policies restricting employee access to the company's calendar or customer contact information." Worse still, the customer information was accessible to ***all*** Freebird employees on their computers and mobile phones for fifteen years, and Freebird had no confidentiality agreements with its employees.[43]

By contrast, in *ABT, Inc. v. Juszczyk*, the district court relied on ABT's Computer Use Guidelines, along with the configuration of its computers, to find that ABT had employed reasonable measures to maintain the confidentiality of its trade secret computer data. The court noted that ABT's Guidelines required "individual employees to utilize computer logins and passwords before access to the system was permitted." The Guidelines also required employees to "periodically perform specific maintenance actions: 'to fulfill ABT data security requirements....'" In addition, each employee was required to indicate understanding and agreement with the Guidelines. The Guidelines and the fact that ABT "1) require[d] a unique login ID and password for employee access; 2) partition[ed] information within the system so as to limit access; and 3) limit[ed] employees' access to particular types of information consistent with the scope of the employee's responsibilities and duties" were found to be sufficient "reasonable measures."[44]

i) Consider Whether To Allow Employees To Use Personal Email Or Personal Devices For Work

Employers must decide whether to allow employees to use their personal email and/or personal devices for work purposes. This can be a very difficult decision as allowing employees to use their own cellphones and personal computers may have significant cost savings for a company. However, it is not without risks.

Some courts have cited an employee's use of his or her personal email, cellphone or personal computer for work purposes as evidence weighing against the employer's protection of its trade secret information.[45] For example, in *Menzies Aviation (USA), Inc. v. Wilcox*, where the employee stored the alleged trade secrets in his personal email and personal computer with the knowledge of his employer, the court found that the employer failed to show that it took reasonable measures to protect the alleged trade secrets.[46] Another district court also cited the fact that employees kept the allegedly trade secret Hardware Book indefinitely on their own personal computers as evidence that the employer did not employ "reasonable measures."[47] Similarly, the district court in *Yellowfin Yachts, Inc. v. Barker Boatworks, LLC*, concluded that Yellowfin had "compromised the efficacy" of its other secrecy efforts by allowing, and even encouraging, its employee Barker to keep the alleged trade secret customer information on his cellphone and personal laptop.[48]

At the same time, other courts have found that employers used "reasonable means" to protect their trade secrets, despite employees storing the trade secrets on their personal cellphones or personal computers where there were other protections in place. For example, in *Vendavo, Inc. v. Long*, employees were allowed to download and store the alleged trade secrets from Salesforce on their personal computers, but only employees with a "need to know" the trade secrets could log in to Salesforce in the first place and those employees were required to sign confidentiality agreements not to disclose the information.[49] In another case, employees were allowed to store the alleged trade secrets on their personal equipment, but only if they obtained approval from senior management first.[50]

In light of the above and their own unique circumstances, employers may choose to require employees to use company email accounts to conduct company business, not personal email accounts. To the extent that employers permit employees to use personal email or devices for work, before permitting remote access to employers' networks from those devices, employers may want to consider the following non-exhaustive list of practical measures to supplement their existing internal policies and procedures:

- Require the devices be equipped with a baseline (or employer-provided) security and virus-protection software, as applicable.
- Require the devices be equipped with the latest manufacturer software updates.
- Require the devices have technology installed so that the employer may remotely wipe data from the device if it is lost or stolen.
- Prohibit employees from downloading or transferring any trade secret or other confidential files to their personal devices. If it is necessary for employees to have such files on their personal devices, require supervisor approval prior to such download or transfer and track which such files are on which employees' personal devices.

j) Consider Monitoring Your Networks And Employees' Compliance With Company Policies And Procedures

Courts cite monitoring of employee access to trade secret information, whether by monitoring employee computer usage, network access or otherwise, as evidence that an employer has taken "reasonable measures" to protect its trade secrets.[51] Similarly, the FBI advises companies to routinely monitor computer networks for suspicious activity in order to deter intellectual property theft.[52] Thus, employers may want to consider some form of routine monitoring of their networks for unauthorized access or other cyberattacks and for other suspicious or unauthorized activity by employees.

k) Provide Comprehensive And Ongoing Training

Employers should consider training employees regarding information security, including identification of the company's trade secrets and how they should be handled, on a regular (at least annual) basis. Training may be less formal at smaller companies, but the goal is the same – anyone with access to trade secrets and other confidential information should understand how to recognize it, its importance and how to handle it. In addition, there may be a need for specialized training for particular groups with regular access to more sensitive or valuable information, or on particular topics (such as how to handle information safely while traveling for work internationally).

In the current crisis, it is important to remind all employees of the new security risks that arise from working-from-home and the need to protect the company's trade secrets. Reminder training may be conducted through interactive video conferencing. Alternatively, companies may send an email highlighting particular concerns raised by working-from-home. Businesses and their IT personnel may also want to keep in regular communication with employees during the current crisis regarding information security measures, malicious schemes, including Covid-19 related attacks, and any network limitations.

As with other measures, the benefits of providing quality training are two-fold. First, regular training on information security and proper handling of trade secrets deters intellectual property theft and decreases the likelihood of loss from innocent, but careless acts as well.[53] Second, some courts have found a lack of such training as evidence that a trade secret owner has not used "reasonable measures" to protect its trade secrets.[54] And, on the flip side, courts will credit such training in conjunction with other evidence of "reasonable measures."[55]

l) Require Employees With Access To Trade Secrets To Sign Confidentiality Agreements

Before employers disclose any trade secrets to employees, employers should consider obtaining executed confidentiality or non-disclosures agreements from those employees. One study of U.S. trade secret litigation found that a court is almost ***25 times*** more likely to find that the trade secret owner has engaged in "reasonable efforts" if it has implemented confidentiality agreements with its employees.[56] While having executed confidentiality agreements with employees alone may not suffice,[57] courts emphasize that having such agreements with any employee who is going to receive trade secret information is an important "reasonable measure."[58] In cases without a non-disclosure agreement, courts have been reluctant to find "reasonable measures" were shown,[59] except where the employee was willful and malicious,[60] or there was a clear showing that other reasonable measures were taken which kept the trade secrets confidential.[61] Thus, as one court recently stated, "[f]ailure to enter into nondisclosure or confidentiality agreements often dooms trade secret claims."[62]

m) Require The Return Of Any Trade Secrets At The Termination Of Employment

To the extent that an employer allows employees to work-from-home or anywhere else outside the workplace, the employer should consider requiring employees to return all trade secret information upon termination of their employment and follow through on that requirement.[63] Not only is this a matter of common sense to secure the company's trade secrets, courts cite this practice as a "reasonable measure" to ensure secrecy.[64] Employers may choose to include this requirement in written agreements with their employees (whether employment agreements, confidentiality agreements, etc.) and may include it in company policies and procedures. In the *Yellowfin Yachts, Inc. v. Barker Boatworks, LLC*, case, for example, the Eleventh Circuit cited Yellowfin's failure to request that Barker return or delete any of the trade secrets as evidence of its lack of "reasonable measures."[65]

n) Take Prompt Action If You Suspect Any Unauthorized Disclosure Of Trade Secrets

If a company learns of, or even suspects, any unauthorized disclosure of its trade secrets or breach of its security protocols, the company should take prompt action in response in order to protect its trade secrets and demonstrate "reasonable measures." Ideally, employers may already have or will develop an Incident Response Plan (IRP) to be followed in the event of a disclosure or breach. Now is a good time to revisit your IRP to assess whether it is flexible enough to deal with an incident during the current crisis with so many of the likely participants working-from-home and to update communications protocols with current remote contact information. Moreover, employers should be aware that if they delay too long in taking action against a trade secret misappropriator, a court may find that they did not take "reasonable steps" to protect their trade secrets and dismiss their trade secret misappropriation claims.[66]

4) Conclusion

Any company with its employees working-from-home in light of the Covid-19 pandemic should ask itself whether it has taken "reasonable measures" to protect its trade secrets in view of the risks posed by that remote workforce. This article addresses some of the myriad steps that a company may take which courts have cited as evidence of "reasonable measures." Each company, however, must evaluate these potential measures, as well as others, through the lens of their own circumstances to create a trade secret protection program that manages risk, protects value and fortifies legal protections. Companies should be

comfortable knowing that they can affirmatively answer the questions posed by the court in *Abrasic 90 Inc. v. Weldcote Metals, Inc.*:

> Did your company employ security measures consistent with your company's assessment of the value of your trade secrets? Does your company take extra measures to ensure the secrecy of its trade secrets above and beyond the company's other business information?[67]

***

If you have any questions about the issues addressed in this article, or if you would like a copy of any of the materials mentioned in it, please do not hesitate to reach out to us.

To view more memoranda, please visit www.quinnemanuel.com/the-firm/publications/
To update information or unsubscribe, please email updates@quinnemanuel.com

---

1 https://www.geekwire.com/2020/zoom-ceo-coronavirus-outbreak-will-change-landscape-work-communication/; https://www.cnn.com/2020/03/20/tech/telework-security/index.html.

2 https://www.law360.com/articles/1250974/motorola-lands-764m-judgment-but-injunction-still-in-the-air.

3 https://www.housingwire.com/articles/42762-amrock-ordered-to-pay-706-million-for-stealing-trade-secrets-from-housecanary/.

4 https://www.law360.com/articles/1106914/asml-secures-223m-jury-verdict-in-trade-secrets-row.

5 For example, venture capitalists spent an estimated $9.3 billion on startups using machine learning and artificial intelligence in 2018. Bloomberg News, "VCs Plowed a Record $9.3 Billion Into AI Startups Last Year," January 8, 2019, https://www.bloomberg.com/news/articles/2019-01-08/vcs-plowed-a-record-9-3-billion-into-ai-startups-last-year; *see also* Towards Data Science, "AI Investment Activity – Trends of 2018," May 26, 2019, https://towardsdatascience.com/ai-investment-activity-trends-of-2018-bf82cd8bd5ea.

6 Uniform Trade Secrets Act §1(4)(i)-(iii) (1985) (adopted in 47 states and the District of Columbia); 18 U.S.C. § 1839(3) (2018). The definitions followed in the other states are based on the Restatement, which provides that "[a] trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it." Restatement (First) of Torts § 757 cmt. b (1939). The Restatement uses the existence of measures to protect the confidentiality of the information as evidence that the information has value and is in fact secret. *Id.*; *see also* Restatement (Third) of Unfair Competition § 39 (1995) ("any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.").

7 *See Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 475 (1974); *Defiance Button Mach. Co. v. C&C Metal Products Corp.*, 759 F.2d 1053, 1063 (2d Cir. 1985).

8 *See Xavian Ins. Co. v. Marsh & McLennan Companies, Inc.*, No. 18CV8273 (DLC), 2019 WL 1620754, at *5 (S.D.N.Y. Apr. 16, 2019); *USM Corp. v. Marson Fastener Corp.*, 379 Mass. 90, 101 (1979); UTSA, § 2 cmt. ("The efforts required to maintain secrecy are those 'reasonable under the circumstances.' The courts do not require that extreme and unduly expensive procedures be taken to protect trade secrets.").

9 *See, e.g., Puroon, Inc. v. Midwest Photographic Res. Ctr., Inc.*, No. 16 C 7811, 2018 WL 5776334, at *7 (N.D. Ill. Nov. 2, 2018) (after noting that "reasonable steps for a two or three person shop may be different from reasonable steps for a larger company," finding that plaintiff small, one-person company's efforts—showing physical prototypes to a limited number of potential customers and granting full access to the prototype's manufacturing specifications only after an NDA was signed—were adequate to protect the trade secrets); *Peggy Lawton Kitchens, Inc. v. Hogan*, 18 Mass. App. Ct. 937, 939 (1984) (where other protective measures were taken, "the absence of admonitions about secrecy or the failure to emphasize secrecy in employment contracts (if there were any in this relatively small business)" was not fatal); *Elm City Cheese Co., Inc. v. Federico*, 251 Conn. 59, 81–86 (1999) (small family-owned company satisfied reasonable efforts requirement where it shared confidential information only with family members and accountant and, further, "kept confidential enough information to make it virtually impossible for its employees to use the rest of the information constituting its trade secret").

10 *United States v. Hanjuan Jin*, 833 F. Supp. 2d 977, 1008 (N.D. Ill. 2012), *aff'd*, 733 F.3d 718 (7th Cir. 2013); *see also, e.g., Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714, 725 (7th Cir. 2003) ("The [Illinois Trade Secrets Act] requires the trade secret owner to take actions that are 'reasonable under the circumstances to maintain [the] secrecy or confidentiality' of its trade secret; it does not require perfection. 765 ILCS 1065/2(d)(2).").

11 *See Colorado Supply Co. v. Stewart,* 797 P.2d 1303, 1306 (Colo. App. 1990) (holding that while measures must be "reasonable under the circumstances to maintain [] secrecy," "[e]xtreme and unduly expensive procedures need not be taken"); *USM*, 379 Mass. at 101.

[12] *See Buffets, Inc. v. Klinke*, 73 F.3d 965, 969 (9th Cir. 1996) (affirming summary judgment for defendant where plaintiff took some "general protective measures" but failed to present evidence that it took reasonable measures "designed to protect the disclosure of" its alleged trade secrets); *see also, e.g., Opus Fund Servs. (USA) LLC v. Theorem Fund Servs.*, LLC, No. 17 C 923, 2018 WL 1156246, at *3 (N.D. Ill. Mar. 5, 2018) (granting motion to dismiss after finding plaintiff did "nothing to differentiate its protective measures for the alleged proprietary trade secrets from those imposed on any other corporate information").

[13] *See BondPro Corp. v. Siemens Power Generation, Inc.,* 463 F.3d 702, 708 (7th Cir. 2006).

[14] Notably, while what is reasonable is judged "under the circumstances," the Covid-19 crisis seems unlikely to provide a significant change in the standard by which "reasonable measures" are judged. Trade secret owners appealing to the current crisis to explain their choices should be able to explain why certain security measures were rendered impossible or made unavailable by the crisis, what security measures were available and why the measures it chose were reasonable under the current circumstances. For example, in *McIntyre v. BP Expl. & Prod., Inc.*, No. 3:13-CV-149 RRB, 2015 WL 999092, at *3–4 (D. Alaska Mar. 5, 2015), *aff'd*, 697 F. App'x 546 (9th Cir. 2017), the plaintiff argued that "the existence of a national emergency excuse[d] his absence of any affirmative efforts to ensure the secrecy of his ideas submitted to Defendants" in connection with Defendants' efforts to contain the uncontrolled oil leak resulting from the Macondo Oil Well explosion in the Gulf of Mexico. The court found that, while "the pressing nature of events and the parties involved may have made a formal confidentiality agreement unreasonable," the plaintiff did not show "reasonable measures" because it did not take any of the available means by which it could have put Defendants on notice and ensured the secrecy of its ideas, such as including language in its communications with Defendants that noted their confidential nature. *Id.* at *3-4.

[15] *See, e.g., Hanjuan Jin*, 833 F. Supp. 2d at 1009 ("The Court concludes that this multi-pronged approach to security—controlled and monitored physical access to Motorola facilities, limited access to the Motorola computer network and Motorola network equipment, a specific policy for the protection of proprietary information, and confidentiality agreements and trainings for Motorola employees—was a reasonable way to maintain the secrecy of the information in Moto 1, Moto 2, and Moto 3.").

[16] *MAI Sys. Corp. v. Peak Comp.,* 991 F.2d 511, 521 (9th Cir. 1993) (noting that reasonable measures include advising employees of the existence of a trade secret); *see also A.F.A. Tours, Inc. v. Whitchurch*, 937 F.2d 82, 89 (2d Cir. 1991) ("[T]he employer must "take appropriate precautions to alert the employee to the need to maintain confidentiality."); *cf. Buffets*, 73 F.3d at 969 (holding that general protective measures were insufficient where employees were not advised of manuals' status as trade secret).

[17] Case No. SA CR 06-92 DOC, 2008 WL 11230384, at *18-19 (C.D. Cal. Feb. 19, 2008).

[18] 898 F.3d 1279, 1300–01 (11th Cir. 2018).

[19] *See, e.g., United States v. Chung*, 659 F.3d 815, 825-26 (9th Cir. 2011), citing UTSA § 1 cmt., 14 U.L.A. 438, 439 (1990) ("As for the second element, reasonable measures for maintaining secrecy 'have been held to include advising employees of the existence of a trade secret, limiting access to a trade secret on [a] 'need to know basis', and controlling plant access.'"); *Brightstar Corp. v. PCS Wireless, LLC*, C.A. No. N18C-10-250 PRW CCLD, 2019 WL 3714917, at *7 (Del. Super. Ct. Aug. 7, 2019) (finding Plaintiff to have made reasonable efforts to maintain confidentiality where it "maintained its pricing information as confidential, stored it in a password protected system, and limited its disclosure only to those with a need to know who are subject to confidentiality"); *Colorado Supply*, 797 P.2d at 1306 (finding sufficiently reasonable measures to secure the confidentiality of information include "advising employees of the existence of a trade secret, limiting access to a trade secret on a 'need to know' basis, and controlling plant access").

[20] *See Vendavo, Inc. v. Long*, 397 F. Supp. 3d 1115, 1137 (N.D. Ill. 2019) ("Here, by limiting access to Salesforce to only those employees who needed it, marking the slide-decks with a confidential legend, and requiring employees who could access the information to sign a confidentiality agreement, Plaintiff has met its burden of taking reasonable measures."); *Brain Injury Ass'n of Cal. v. Yari*, No. CV 19-5912-MWF (JCX), 2019 WL 4544419, at *4 (C.D. Cal. Aug. 9, 2019) (finding reasonable measures would be shown if Master List was stored in a secure CRM database with access restricted to only two BIACAL members, including Ms. Yari, and her "access was strictly limited for the purposes of migrating the Master List data to BIACAL's new database"); *ABT, Inc. v. Juszczyk*, No. 5:09CV119-RLV, 2010 WL 3156542, at *5 (W.D.N.C. Aug. 10, 2010) (noting reasonable measures included "ABT's computers were configured in such a way as to 1) require a unique login ID and password for employee access; 2) partition information within the system so as to limit access; and 3) limit employees' access to particular types of information consistent with the scope of the employee's responsibilities and duties"); *Hanjuan Jin*, 833 F. Supp. 2d at 1008-09 ("Motorola also had measures in place to protect confidential and proprietary information internally, including restricting access within the Motorola network depending on the user's authorization and the classification status of a document or file.").

[21] David S. Almeling et al., "*A Statistical Analysis of Trade Secret Litigation in Federal Courts*," 45:2 Gonzaga L. Rev. 291, 323 n.130 (2010), available at http://blogs.gonzaga.edu/gulawreview/files/2011/01/AlmelingSnyderSapoznikowMcCollumWeader.pdf.

[22] *See* https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view.

[23] *See, e.g., nClosures Inc. v. Block & Co.*, 770 F.3d 598, 602 (7th Cir. 2014) (finding nClosures did not take reasonable steps to protect its confidential drawings where confidentiality agreements were not signed, the confidential

drawings were not marked "confidential" or equivalent, and "the drawings were not kept under lock and key, nor were they stored on a computer with limited access").

[24] 80 F. Supp. 3d 900, 912 (C.D. Ill. 2015) (also noting that defendant "kept customer information in folders on the top of [his] desk," which were "accessible to anyone in the building including other employees and even custodians").

[25] *Protection Techns., Inc. v. Ribler,* No. 3:17-cv-00144-LRH-WGC, 2017 WL 923912, at *1–2 (D. Nev. Mar. 8, 2017) (finding plaintiff took reasonable measures by "requiring employees to sign confidentiality agreements and limiting access to the data to password-protected entry points"), citing *MAI*, 991 F.2d at 521; *see also, e.g., Chartwell Staffing Servs. Inc. v. Atl. Sols. Grp. Inc.*, No. 8:19-CV-00642-JLS-JDE, 2019 WL 2177262, at *6 (C.D. Cal. May 20, 2019) ("Chartwell has shown that it has taken reasonable measures to keep the information in the MOS and CRM databases secret. Employees must use a password to access the databases, their credentials are immediately deleted upon termination or resignation, and each employee must sign an Employment Agreement that prohibits the disclosure of information contained in MOS and CRM."); *Bartech Sys. Int'l, Inc. v. Mobile Simple Solutions, Inc.*, No. 2:15–cv–02422–MMD–NJK, 2016 WL 3002371, at *6 (D. Nev. May 24, 2016) (deciding an alleged trade secret was confidential because it was "kept within a password-protected, internal server, and only [plaintiff's] own developers had access to it"); *PQ Labs, Inc. v. Yang Qi*, No. 12-0450 CW, 2014 WL 334453, at *3 (N.D. Cal. Jan. 29, 2014) (finding reasonable measures where company "relies on passwords and firewalls to protect its electronic information").

[26] *Maxpower Corp. v. Abraham*, 557 F. Supp. 2d 955, 961 (W.D. Wis. 2008).

[27] *See, e.g., United States v. Zhang*, 590 F. App'x 663, 665 (9th Cir. 2014) (finding reasonable measures taken where "Marvell 'advis[ed] [users] of the existence of a trade secret, limit[ed] access to [the] trade secret on [a] 'need to know basis,' and controll[ed] . . . access' to the extranet by requiring usernames and passwords, additional passwords and licenses for certain documents, and the user's agreement to a Terms of Use"); *Lux Glob. Label Co., LLC v. Shacklett*, No. CV 18-5061, 2019 WL 3530424, at *4 (E.D. Pa. July 31, 2019) (finding reasonable measures taken, even in absence of non-disclosure agreement, where plaintiff was "storing sensitive files on separate network drives with restricted access through individual login and password protection, limiting information access to high-level employees and officers only, prohibiting non-employees' unsupervised access to non-public areas of their offices, and monitoring employee telephone and computer usage").

[28] *See SKF USA Inc. v. Bjerkness*, Nos. 08 C 4709, 09 C 2232, 2010 WL 3155981, at *6 (N.D. Ill. Aug. 9, 2010) (finding plaintiff took reasonable efforts to maintain the secrecy of its information where it (1) required employees to sign secrecy agreements, (2) implemented password protection for important files and granted access to different sets of documents based on employees' duties, (3) instructed employees not to share its databases with customers, (4) and only shared information with customers after having the customer sign a nondisclosure agreement); *Extreme Reach, Inc. v. Spotgenie Partners, LLC*, No. CV 13–07563–DMG (JCGx), 2013 WL 12081182, at *4 (C.D. Cal. Nov. 22, 2013) (finding plaintiff "established that it took reasonable steps to maintain the secrecy of its Customer list by password protecting it, making it available to only certain employees, and protecting it with a firewall"); *cf. Boston Laser, Inc. v. Zu*, No. 3:07-CV-0791, 2007 WL 2973663, at *10, *12 (N.D.N.Y. Sept. 21, 2007) (finding that plaintiff had not taken reasonable measures to preserve secrecy where, among other things, "the computer network on which such matters are digitally stored is generally not even password protected beyond the log-in process").

[29] *See, e.g., PQ Labs*, 2014 WL 334453, at *3 (finding reasonable measures where company "relies on passwords and firewalls to protect its electronic information"); *Extreme Reach*, 2013 WL 12081182, at *4 (citing protection of Customer List with a firewall as one of reasonable measures); *Wrap–N–Pack, Inc. v. Eisenberg,* No. 04-cv-4887, 2007 WL 952069, at *9 (E.D.N.Y. Mar. 29, 2007) (company implemented significant safeguards to protect information by, among other things, installing firewalls and security software).

[30] 2008 WL 11230384, at *17.

[31] *Id.* at *17-18. However, the district court stated that Broadcom's security measures were "not great," citing "deficiencies" in its communication of what information was confidential to its employees, a failure to train employees how to handle such information, and a lack of "a comprehensive system in place for designating which documents were and which documents were not confidential." *Id.*

[32] *See, e.g., Aetna, Inc. v. Fluegel*, No. CV074033345S, 2008 WL 544504, at *5 (Conn. Super. Ct. Feb. 7, 2008) (commenting on plaintiff's use of encryption for some documents as evidence of its reasonable measures to maintain secrecy).

[33] According to one study, 69% of employees have not changed the default password on their home Wi-Fi router. *See* Bruce Sussman, Coronavirus and Cybersecurity: Remote Workforce Risks to Track, *Secureworld Expo* (Mar. 12, 2020), citing 2020 State of the Phish, available at https://www.secureworldexpo.com/industry-news/coronavirus-and-cybersecurity-remote-employee-risk.

[34] *See, e.g., Morlife, Inc. v. Perry*, 56 Cal. App. 4th 1514 (1997) ("While labeling information 'trade secret' or 'confidential information' does not conclusively establish that the information fits this description, it is nonetheless an important factor in establishing the value which was placed on the information and that it could not be readily derived from publicly-available sources.") (citations omitted); *Vendavo*, 397 F. Supp. 3d at 1137; *Picker Int'l Corp. v. Imaging Equip. Servs., Inc.*, 931 F. Supp. 18, 30 (D. Mass. 1995); *see also* Almeling et al., supra at 321-24.

[35] As a necessary step to prevail on a claim under the Uniform Trade Secrets Act, a trade secret owner may need to show that the misappropriator had "reason to know" that it was not free to use the trade secret. UTSA § 1(2) (1985).

[36] *See, e.g., PQ Labs*, 2014 WL 334453, at *4 (finding reasonable measures shown absent any marking because "PQ Labs has presented evidence that it used other means to notify its employees and agents that its technological and customer information was confidential").

[37] *See, e.g., Yellowfin Yachts*, 898 F.3d at 1300-01 (holding that Yellowfin had failed to reasonably protect information as a trade secret under Florida law where, among other things, Yellowfin did not "mark[] the Customer Information as confidential"); *Jensen v. Redevelopment Agency of Sandy City*, 998 F.2d 1550, 1557 (10th Cir. 1993) (no trade secret where allegedly secret design and information not marked as confidential); *Hoffman v. Impact Confections, Inc.*, 544 F. Supp. 2d 1121, 1126 (S.D. Cal. 2008) (granting summary judgment on trade secret claim because information was not designated "confidential" as required by NDA); *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1335 (N.D. Ga. 2007) (holding that Diamond Power did not show reasonable efforts where, among other things, it did not introduce any evidence that it "labeled the file confidential"); *Alagold Corp. v. Freeman*, 20 F. Supp. 2d 1305, 1315–16 (M.D. Ala. 1998), *aff'd*, 237 F.3d 637 (11th Cir. 2000) (finding Alagold did not show reasonable efforts where, among other things, there was "no evidence that Alagold's proprietary information was marked 'confidential'"); *Web Commnc'ns Group, Inc. v. Gateway 2000, Inc.*, 889 F. Supp. 316, 320 (N.D.Ill. 1995) (granting summary judgment under the Illinois UTSA in part because plaintiff failed to protect the confidentiality of an advertising insert by stamping or designating it as confidential); *Convolve Inc. v. Compaq Computer Corp.*, 527 F. App'x 910 (Fed. Cir. 2013) (finding that the information lost any "trade secret status" when it was disclosed without markings required under the non-disclosure agreement); *SortiumUSA LLC v. Hunger*, No. 3:11-cv-1656-M, 2013 WL 11730655, at *23 (N.D. Tex. March 31, 2013) (granting a motion to dismiss where alleged trade secret drawings did "not bear any restrictive warning as to their alleged confidentiality or instructions to the persons working on them to safeguard their alleged secrecy"); *Nike Inc. v. Dixon*, No. CV 01-1459-BR, 2004 WL 1845505, at *4 (D. Or. Apr. 6, 2004), *aff'd*, 163 F. App'x 908 (Fed. Cir. 2006) (granting summary judgment to defendant where plaintiff failed to mark materials or otherwise take measures to protect secrecy); *Triton Const. Co. v. E. Shore Elec. Servs., Inc.*, No. CIV.A. 3290-VCP, 2009 WL 1387115, at *22 (Del. Ch. May 18, 2009), *aff'd,* 988 A.2d 938 (Del. 2010) (finding no reasonable measures where plaintiff failed to mark documents as secret or confidential and never conducted training or provided instructions to its employees on information that the company considered secret or confidential).

[38] *See* https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view.

[39] The FBI has identified "[u]ndefined policies regarding working from home on projects of a sensitive or proprietary nature" as a factor which may increase intellectual property theft. *See* https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view.

[40] The design and implementation of a comprehensive set of policies and procedures is highly fact-specific and is beyond the scope of this article.

[41] *See, e.g., J.H. Wright & Assocs., Inc. v. Engerson*, No. CR. A. 00-0906RVL, 2000 WL 1848135, at *8 (S.D. Ala. Dec. 1, 2000) (finding reasonable measures not established where "written policy generally requiring confidentiality" did "not list manufacturer drawings or bill of materials as covered documents"); *Enter. Leasing Co. v. Ehmke*, 197 Ariz. 144, 151 (Ct. App. 1999) (holding that a company took reasonable measures to protect its trade secrets by, among other things, including a confidentiality provision in the employee policy handbook, which all employees were required to acknowledge and sign); *Menzies Aviation (USA), Inc. v. Wilcox*, 978 F. Supp. 2d 983, 995 (D. Minn. 2013) (finding reasonable measures not shown because, among other reasons, plaintiff did not provide defendant employee with "a policy designating the information as confidential"); *Wrap–N–Pack,* 2007 WL 952069, at *9 (finding reasonable measures where, among other things, "WNP distributed an employee policy-and-procedure manual to all employees that contained a code of conduct defining unacceptable behavior to include disclosing confidential information about its customers to competitors and others" and "reminded salesmen of their duty and obligation to maintain customer confidentiality via office memoranda").

[42] *See Abrasic 90 Inc. v. Weldcote Metals, Inc.*, 364 F. Supp. 3d 888, 899 (N.D. Ill. 2019) ("The confidentiality language in the employee handbook stating that employees are 'not to reveal or discuss information about CGW, its customers or its employees when outside the company' is too broad and vague to confer meaningful protection over the information at issue.").

[43] No. 2:18-CV-02026-HLT, 2019 WL 5964583, at *5 (D. Kan. Nov. 13, 2019).

[44] *ABT*, 2010 WL 3156542, at *5.

[45] *See Coihue, LLC v. PayAnyBiz, LLC*, No. 17-24062-CIV, 2018 WL 7376908, at *5 (S.D. Fla. Feb. 6, 2018) (on a motion to dismiss under DTSA and Florida UTSA, Defendants argued that Plaintiffs failed to make reasonable efforts to maintain the secrecy of the trade secrets because they allowed storage of trade secrets on employee's personal computer and cell phone).

[46] *Menzies Aviation*, 978 F. Supp. 2d at 995.

[47] *Diamond Power*, 540 F. Supp. 2d at 1335.

[48] *Yellowfin Yachts*, 898 F.3d at 1300-01.

[49] *Vendavo*, 397 F. Supp. 3d at 1137.

[50] *See, e.g., Intertek Testing Servs., N.A., Inc. v. Pennisi*, No. 19-CV-7103 (SJF)(ARL), 2020 WL 1129773, at *18 (E.D.N.Y. Mar. 9, 2020).

[51] *See, e.g., Orthofix Inc. v. Hunter*, 55 F. Supp. 3d 1005, 1013 (N.D. Ohio 2014), rev'd on other grounds and remanded, 630 F. App'x 566 (6th Cir. 2015) ("[I]n this case, where there were no reasonable efforts to enforce the clause or monitor the allegedly protected information gathered by employees, the provisions in the employee agreement, handbook, and Code of Conduct are insufficient."); *Diamond Power*, 540 F. Supp. 2d at 1335 (holding that Diamond Power did not show reasonable efforts because its failure to track or regulate use of the Hardware Book meant that employees could retain it indefinitely on their own computers); *Lux Glob.,* 2019 WL 3530424, at *4 (citing "monitoring employee telephone and computer usage" among other reasonable measures taken by plaintiff); *Hanjuan Jin*, 833 F. Supp. 2d at 1008-09 ("Users of the Motorola network were reminded every time they logged onto the Motorola network that their use of the network was subject to monitoring, and that it could only be used for authorized purposes.").

[52] *See* https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view. The FBI has also identified factors for employers to look for to determine if an employee may be an internal threat: greed or financial need, disgruntlement at work, allegiance to another company or country, vulnerability to blackmail, an "above the rules" attitude, vulnerability to the promise of a better job, drug abuse or alcohol abuse, and/or family problems. *Id.*

[53] The FBI advises organizations to "[e]ducate and regularly train employees on security or other protocols" to deter intellectual property theft, and identifies a lack of employee training "on how to properly protect proprietary information" as an organizational factor which may increase the ease for thievery. *See* https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view.

[54] *See, e.g., AW Dynamometer Inc. v. Manley*, No. 07-CV-1307, 2007 WL 9734955, at *5 (C.D. Ill. Nov. 29, 2007) (finding plaintiff's "affirmative measures" used to keep the material secret fall short where "[t]here was no special training used to inform Plaintiff's employees that the list was confidential nor were people who had access to the information, customers or sales representatives, informed that the information was secret"); *Triton Const.*, 2009 WL 1387115, at *22 (finding no reasonable efforts to keep secret where plaintiff did not mark trade secrets as "secret or confidential, and never conducted any training or provided any instructions to its employees on information that the Company considered secret or confidential").

[55] *See, e.g., Wyeth v. Natural Biologics, Inc.,* 395 F.3d 897, 899–900 (8th Cir. 2005) (holding that, under Minnesota's UTSA, the plaintiff had implemented reasonable measures by limiting access to confidential information, training employees, controlling documents, and obtaining oral and written understandings of confidentiality); *Intertek Testing*, 2020 WL 1129773, at *18 (finding Intertek took reasonable measures where, among other things, it required employees "to participate in annual compliance and code of ethics training").

[56] Almeling et al., supra at 322 n.128.

[57] *See Diamond Power*, 540 F. Supp. 2d at 1335 (finding Diamond Power did not show reasonable efforts despite requiring its employees to sign a general confidentiality agreement upon the commencement of their employment because it had a "demonstrated ability to be more restrictive over information which it wished to keep secret," and had other security measures available but did not employ them); *AmeriGas Propane v. T-Bo Propane, Inc.,* 972 F. Supp. 685, 701 (S.D. Ga. 1997); *Equifax Servs., Inc. v. Examination Mgmt. Servs, Inc.*, 216 Ga. App. 35 (1994) (the existence of a confidentiality agreement without any further steps to maintain secrecy of trade secrets was insufficient to avoid summary judgment).

[58] *See, e.g., MAI,* 991 F.2d at 521 (holding plaintiff had taken reasonable measures to maintain the secrecy of its customer database by "requir[ing] its employees to sign confidentiality agreements respecting its trade secrets"); *Chung*, 659 F.3d at 825–26 (citing employee confidentiality agreements as a security measure often considered among reasonable measures); *RKI, Inc. v. Grimes*, 177 F. Supp. 2d 859, 866 (N.D. Ill. 2001) (granting preliminary injunction where plaintiff only provided information to employees on a need-to-know basis, maintained the security of the information through "such means as limited access and password-protected computer databases," and required employees to sign employment agreements or acknowledge the receipt of employee handbooks that contained non-disclosure clauses); *PQ Labs*, 2014 WL 334453, at *3; *Vendavo*, 397 F. Supp. 3d at 1136-37; *SKF*, 2010 WL 3155981, at *6; *Xantrex*, 2008 WL 2185882, at *18 (finding reasonable measures where Xantrex had employees sign non-disclosure agreements because "[t]he existence of a nondisclosure agreement puts the employee on notice that the computer programs of an employer are considered trade secrets"); *S&S Computers & Design, Inc. v. Paycom Billing Services, Inc.*, No. 5:00-CV-00058, 2001 WL 515260 (W.D. Va. April 5, 2001) (holding reasonable measures alleged where trade secrets in software, hardware and documents protected by implementing password protection, physical locks, limited access and non-disclosure agreements); *Enter. Leasing*, 197 Ariz. at 151 (finding reasonable measures where company adopted general directives regarding confidentiality, including a confidentiality provision, in its employment agreements with high level managers and included a confidentiality provision in the employee policy handbook, which all employees were required to acknowledge and sign).

[59] *Yellowfin Yachts*, 898 F.3d at 1300-01 (holding Yellowfin did not take reasonable measures, despite placing the trade secrets on a password-protected computer network and limiting employee access, where defendant Barker "refused to sign an employment agreement which stated that he would, among other things, keep all Yellowfin trade secrets in confidence").

[60] *See Alagold*, 20 F. Supp. 2d at 1315–16 (finding Alagold did not show reasonable measures where, among other things, Alagold gave Freeman "full access to all of Alagold's confidential information, [but] did not require Freeman to execute a confidentiality or non-compete agreement limiting the use of information Freeman learned during his employment with Alagold").

[61] *See Lux Glob.*, 2019 WL 3530424, at *4 (finding non-disclosure agreement with employee not required to show "reasonable measures" to protect trade secrets where employee's behavior was willful and malicious); *Nelson Bros. Prof'l Real Estate LLC v. Jaussi*, No. SACV170158DOCJCGX, 2017 WL 8220703, at *6 (C.D. Cal. Mar. 23 2017) (finding reasonable measures despite lack of non-disclosure agreement with defendant where (1) plaintiff placed the secrets on a password protected, shared computer drive that could only be accessed from plaintiff's office and limited access to only 7-10 employees, (2) when the defendant was suspended, plaintiff sent him an email telling him not to misappropriate any trade secrets, and (3) when defendant was terminated, plaintiff sent him another email telling him to return all of plaintiff's property in his possession).

[62] *Abrasic 90*, 364 F. Supp. 3d at 898.

[63] There are many important considerations to keep in mind to protect trade secrets upon the termination of an employee's employment, but those considerations are beyond the scope of this article. If you would like additional information regarding best practices for the final stages of the employee life cycle, including off-boarding and post-employment, please feel free to contact us.

[64] *See, e.g.*, *Orthofix*, 55 F. Supp. 3d at 1013; *Intertek Testing*, 2020 WL 1129773, at *18.

[65] *Yellowfin Yachts*, 898 F.3d at 1300.

[66] For example, in *HiRel Connectors, Inc. v. United States*, the district court granted summary judgment for the defendant where the plaintiff had waited ***more than two years*** after it learned that its trade secrets had been published online to file suit, concluding that the information ceased to be a trade secret. No. CV01–11069 DSFVBKX, 2005 WL 4958547, at *5 (C.D. Cal. Jan. 1, 2005); *see also, e.g., Alamar Biosciences, Inc. v. Difco Labs., Inc.*, No. CIV-S-941856 DFL PAN, 1995 WL 912345, at *6 (E.D. Cal. Oct. 13, 1995) (finding failure to "bring suit, or even approach and warn" defendant of its claims for "over four years" established that plaintiff did not take reasonable steps to protect its trade secrets and granting summary judgment to defendant). In *PQ Labs, Inc. v. Yang Qi*, the district court found that waiting ***twenty months*** to file suit after learning of defendants' possible misappropriation was reasonable where, unlike *HiRel Connectors*, the trade secrets were not published online. *PQ Labs*, 2014 WL 334453, at *4. On the other hand, in *Pre-Paid Legal Servs., Inc. v. Harrell*, concluding that the plaintiff had taken "reasonable measures," the court noted, among other things, that the plaintiff had made a regular practice of taking action against breaches, sending cease and desist letters and entering into agreed injunctions against former employees who had misappropriated trade secrets. No. CIV-06-019-JHP, 2008 WL 111319, at *11-12 (E.D. Okla. Jan. 8, 2008).

[67] *See Abrasic 90*, 364 F. Supp. 3d at 902–03 (finding plaintiff did not employ reasonable measures because its answer to these questions was "plainly no").