PRESERVING YOUR COMPANY'S CONFIDENTIAL BUSINESS INFORMATION

in the Age of Working Remotely and Cybersecurity Threats

Brian Whiteley, Michael Murphy, and **Payne Horning** Barclay Damon LLP

All businesses have information they consider confidential. Many expect the use of confidentiality and nondisclosure agreements with business partners, vendors, and employees—as well as trade secret and fair competition laws—to protect that confidential information. The assumption is correct, to a degree, but protecting confidential business information requires a comprehensive plan and consistent overview, with periodic assessments and updating. Those companies that fail to remain vigilant, particularly as more and more employees work remotely, can find themselves at the mercy not only of bad actors but of the law, which demands careful safeguarding to protect confidential information.

In one recent case in Delaware,[1] a court denied a company's attempt to enjoin another business from competing with it because some of the alleged confidential information had been shared on videoconference calls that were not sufficiently guarded. The company had failed to take basic steps to police who joined the calls by requiring passwords for entry, admitting participants from a virtual waiting room into the call individually, or taking roll call at the start of the meetings. Despite the fact that the company had required some participants on the videoconference calls to sign nondisclosure agreements, others who had joined could not be identified let alone confirmed to have signed binding contracts. Because the company could not demonstrate that it met its own burden to protect the alleged trade secrets, the court declined to halt the competitor's operations.

While the lessons of this case may not be new—businesses have always had to implement measures to protect confidential information—the circumstances are emblematic of a changing landscape. More employees are working remotely, widening the avenues for trade secrets and other valuable business assets to become compromised. Additionally, companies are increasingly at risk of sophisticated cyberattacks. The U.S. Department of Justice reported in 2020 that Massachusetts-based vaccine developer Moderna, Inc. was the victim of a Chinese government–linked hack.

So, what should you do to protect your information? First, understand what a trade secret is and identify your confidential information. Second, design a comprehensive plan to protect the information, understanding the need to play defense. Third, recognize the importance of the human element and how to guard against mistakes, particularly in the digital age. Fourth, be sure to stay on top of your protection plan with consistent and thorough reviews (i.e., at least on an annual basis). And finally, if there has been a breach, act quickly.

WHAT CONSTITUTES A TRADE SECRET?

Trade secrets come in all shapes and sizes: formulas, patterns, compilations, methods, techniques, processes, devices, etc. Whatever the form, the key is that a trade secret involves something not generally known or available to the public or readily ascertainable by other means. If the public knows the "secret sauce," odds are your claim will be unsuccessful. In one case,[2] the fact that recipes a party sought to protect had been published in the *New York Times* weighed against the recipes' characterization as trade secrets. Most broadly, trade secrets can be thought of as something that gives the possessor some kind of an economic edge over its competitors, whether actual or potential.

Identifying what information qualifies for protection under state and federal law is the first step in preparing a comprehensive plan. Once known, the next step is actually developing that plan.

WHY YOU NEED TO PLAY DEFENSE

Developing a plan to protect confidential information requires a holistic approach. Today, all plans must include an adequate cybersecurity program, including up-to-date encryption and antivirus software. Internally, organizations should restrict the availability of electronic information to those with

a need to know. Payroll employees do not need access to engineering plans; engineers likely do not need information concerning new sales strategies.

But don't lose sight of the basics—protect physical space through locks, posted notices, and restricted-access places. Have secure disposal methods for sensitive documents and electronic files. Have nondisclosure agreements with third parties forbidding unauthorized use and disclosure of confidential information and be sure to get those agreements in place before disclosing any confidential information.

Taking steps like these to protect a trade secret are not just advisable, they are crucial—not only for your business in general but to succeed in any litigation brought to protect the information. One required element in a misappropriation claim is convincing a court the organization took reasonable measures to safeguard the information. What is reasonable will vary with the particular circumstances, with courts potentially requiring more of larger, more sophisticated organizations than smaller ones.

WHY THE HUMAN FACTOR IS SO CRITICAL

Perhaps the biggest threat to sensitive information comes from disclosure by employees with access during their employment. The disclosures can be innocent, arising from a lack of education or inattentiveness, particularly with the increasingly sophisticated tools and ploys designed by hackers—or intentional, arising from an employee taking the company's confidential information to compete. Whatever the reason, businesses should take steps to protect against employee misuse.

Businesses can shore up the risk of employee disclosures by maintaining policies concerning access to confidential information, including prohibitions on sharing confidential information with those who don't have a need to know. Employees should be educated regarding the need to keep information confidential wherever they are. No business wants to learn its strategic business plans were left in a hotel while an employee worked off-site. One of the best defenses against this particular risk is having your employees sign confidentiality and nondisclosure agreements. These contracts not only provide a record of your efforts, but they can also serve as convincing evidence in court. Last year, an individual seeking an injunction in a trade secrets case[3] fell short because of a lack of any agreement limiting the use or disclosure of the proprietary property at issue. While the court acknowledged the individual had limited access to where the information was stored internally and monitored who used it, the court found the failure to have a nondisclosure or licensing agreement in place limiting the use of the information fatal.

When an employee has signed a confidentiality agreement, the employer can claim breach of contract. And while it is always best to have an agreement in place—even in the absence of an agreement—the employer may have other remedies, including trade secret claims.

WHY YOU NEED AN ANNUAL REVIEW

Protecting confidential information is not a one-time project or investment; it is an essential and ongoing component of a business's day-to-day operations. To that end, companies should incorporate a continual monitoring program to ensure those with access to their trade secrets are preserving them. This can take the form of an annual review of what confidential material the business owns and what protections have been taken to preserve it. Moreover, the review should take into account developments or other changes that may have taken place with the technology or programs that are used to safeguard the confidential information. The annual review also provides a good opportunity to review employee files to ensure each member of the staff who comes into contact with confidential information has signed a nondisclosure agreement and that each of those contracts is up to date.

Employers also need to implement a process for when employees depart. Each staff member who has had access to trade secrets should be asked about their post-exit plans. Additionally, it is crucial to remind them about their contractual obligations, noting the legal consequences if not abided.

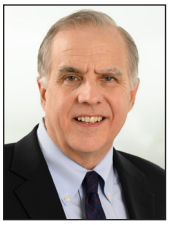
HOW PROMPT ACTION CAN MAKE A DIFFERENCE

In the digital age, misappropriated confidential information can be shared with the click of a button. Thus, the harm from losing the information begins immediately, and businesses seeking to protect that information must act quickly.

To ultimately prevail in court, the business will need to satisfy a potentially skeptical judge up front that: (1) the information is truly confidential, (2) the business has taken reasonable measures to protect it, and (3) information was taken by improper means. However, it is often the case that asking for a preliminary injunction is the very first step. To obtain a preliminary injunction, a plaintiff must demonstrate (1) a likelihood of success on the merits, (2) a threat of irreparable harm if an injunction is not granted, (3) that the balance of the equities favors the issuance of an injunction, and (4) if the injunction is granted, it will not disserve the public interest.

How soon a company actually moves for the injunction can be just as important as how they make the case for one. Unreasonable or unnecessary delay can weigh against an argument that the threat is significant enough for immediate court intervention.

Confidential information is critically important to many businesses. Protecting it requires careful planning, diligence, vigilance, and prompt action when there is an issue.



Brian Whiteley is a partner and Commercial Litigation Practice Group leader at Barclay Damon LLP. He concentrates his practice on complex commercial litigation, representing corporate and individual clients in trade secret and noncompetition matters, software licensing and intellectual property disputes, contract actions, employment discrimination suits, and wrongful termination suits.

Michael Murphy is a partner at Barclay Damon LLP. He handles complex litigation with an emphasis on labor and employment, municipal, and civil rights and constitutional law. Michael's clients are local and national leaders in business, government, and community organizations. He frequently represents clients in sensitive, high-profile litigation and investigations.

Payne Horning is an associate at Barclay Damon LLP. He concentrates his practice on advising and representing clients on a wide range of labor and employment matters, including employment litigation, and advising clients on issues such as hiring, discipline, and termination, among other things.

1 See *Smash Franchise Partners, LLC v. Kanda Holdings, Inc.*, No. 2020-0302-JTL, 2020 Del. Ch. LEXIS 263 (Ch. Aug. 13, 2020).
2 See *WGJ Holdings, Inc. v. Greenberg*, No 07 Civ. 2742, 2008 U.S. Dist. LEXIS 850, 2008 WL 80932 (S.D.N.Y. Jan. 8, 2008).
3 See *Mason v. AmTrust Fin. Servs.*, 848 F. App'x 447 (2d Cir. 2021).