Protecting Trade Secrets in Remote and Hybrid Workplaces: 3 Questions Employers Should Be Asking Themselves

Insights
9.30.22

Employers today are coming to terms with what has developed into full-time remote or hybrid work arrangements for many workers. However, you should recognize that the rise of these work arrangements may create additional security risks for your trade secrets and other confidential business information, particularly when employees leave your company to work for a competitor. Therefore, you should consider taking steps to identify trade secrets and consistently enforce reasonable security measures for all employees. Here are three questions to ask as you create an action plan to protect your trade secrets.

1. Have You Identified the Risks?

The remote and hybrid workforce is still shifting as companies create new policies in light of the ever-evolving COVID-19 landscape. According to a recent Gallup poll, 29% of employees in "remote-capable" jobs were working from home full time in June — down from 39% in February. Notably, however, the share of employees working hybrid schedules is still on the rise.

Workers in the "technology, communications, professional services, and finance and insurance" sectors are experiencing "the highest rates of remote work," according to a recent *Washington Post* article, but the data also shows "remote work growing across the board."

While the percentage of employees working remotely on a full-time basis is down from its pandemic peak, it remains well above its pre-pandemic level. In fact, according to Gallup, only 8% of people in "remote-capable" roles were working from home in 2019. The move to increased full-time remote work and hybrid work schedules has dovetailed with talent shortages and the so-called "Great Resignation," which saw a record 47.4 million workers voluntarily quit their jobs in 2021, according to the Bureau of Labor Statistic.

These trends have carried over to 2022. In fact, the latest "Job Openings and Labor Turnover Survey" (JOLTS) from the Bureau of Labor Statistics for July 2022 showed total hires outpacing total separations by some 500,000 and quits outpacing layoffs and discharges by a three-to-one margin.

These factors can create a perfect storm for an uptick in trade secret misappropriation. For example, in a tight labor market filled with remote workers and recruiters vying for skilled job

candidates, employees may be entertaining multiple new opportunities under the radar and during work hours. Moreover, they might be using your trade secrets for their own competitive benefit.

Since most trade secret misappropriation takes place around the time an employee leaves a company to go to work for a direct competitor, remote workers may pose a greater risk to employers in this regard. Therefore, safeguarding your trade secrets is more critical than ever.

2. Do You Know What Qualifies as a Trade Secret?

Employers need to understand what confidential and proprietary business information owned by the company qualifies as a trade secret. The federal Defend Trade Secrets Act (DTSA) defines a "trade secret" 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:

- The owner thereof has taken reasonable measures to keep such information secret; and
- 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.

3. Do You Have an Effective Plan to Protect Your Information?

Given the prevalence of full-time remote work, hybrid work schedules, and employee-initiated separations, what can employers do to guard their trade secrets and other confidential business information?

Under DTSA — and state Uniform Trade Secret Acts — employers must take reasonable security measures to keep their trade secrets "secret." This generally means taking steps such as the following:

- Implementing written confidentiality policies;
- Requiring new hires and existing employees to execute nondisclosure agreements;
- Maintaining well-defined computer and network security policies that limit access to information on a "need to know" basis; and
- Prohibiting the unauthorized downloading, uploading, sharing, and use of company owned data.

These reasonable security measures must apply to all employees regardless of their work location. Also, you must consistently enforce compliance with your written policies. Employers must also

Also, you must consistently enforce compliance with your written policies. Employers must also maintain regular contact with remote employees and require them to participate in business meetings and other employer activities — through video conferencing or chat apps or in person — as needed.

When an employee gives notice that they are departing, regardless of work location, employers can take steps to prevent or undercover trade secret misappropriation. Steps may include, but are not limited, to the following:

- Monitoring e-mail traffic and computer access for unusual activity.
- Conducting exit interviews and recovering and examining all company property issued to the employee, including laptop computers, phones, and other devices.
- Obtaining a return-of-property declaration.
- Writing a letter to remind the departing employee of confidentiality and other contractual obligations owed to the employer.
- Terminating access to computer assets and accounts as soon as the employee departs or earlier if needed.

In short, while remote and hybrid work arrangements may expose employers to an enhanced risk of trade secret misappropriation, taking the following steps on the front-end can minimize the risks of trade secret misappropriation when an employee departs:

- Identify trade secrets;
- Create, implement, and consistently enforce reasonable security measures for all employees;
- Maintain regular engagement with remote workers; and
- Conduct thorough exit interviews and off-boarding procedures to ensure data is protected.

Conclusion

We will continue to monitor the latest developments related to trade secrets and confidential business information, so you should ensure you are subscribed to Fisher Phillips' Insight system to gather the most up-to-date information. If you have questions, please contact the author of this Insight, your Fisher Phillips attorney, or any attorney in our Employee Defection and Trade Secrets Practice Group.

Related People

Greg Grisham
Partner
901.333.2076
Email

Service Focus

Counseling and Advice

Employee Defection and Trade Secrets