PROTECTION OF TRADE SECRETS IN THE MODERN WORKPLACE

Some suggestions on how to safeguard confidential company information.

BY JOHN EASTWOOD

When it comes to your company's sensitive non-public information, it's an important first step to make sure that employees and management are both part of a protective culture. Too often non-disclosure agreements (NDAs) or confidentiality terms are simply tucked away within a bunch of formal documents that are hastily signed at the time of hiring – but with little or no discussion later on.

Instead, communications about the company's expectations need to be made crystal clear from the outset. Explicit rules and procedures that everybody understands should be in place regarding the treatment of sensitive confidential information.

Typical rules might include:

- No private drives, USBs, computers, etc. allowed in the office premises or used for company business.
- Physical or electronic access to your trade-secrets information is restricted to those who really need to see it.
- Only software approved by the company may be installed, with the installation done by the company.
- Use of private messaging and email software to communicate from work computers is prohibited or restricted.
- When documents are confidential, employees must mark them (or use document templates that include such markings) stating the confidential nature of the documents.
- A company-wide "clean desk" policy must be maintained.
- Additional security measures beyond mere passwords may be mandated to access systems, including verification software, fingerprint readers, etc.

Whatever rules you implement, they should be communicated clearly and unambiguously to the employees and management. An annual or even quarterly security meeting with employees to review the requirements is a good way to ensure that employees know what they are expected to do. Sign-offs, quizzes, and acknowledgements can help make sure that the personnel are not simply "going through the motions" without paying close attention.

Companies should also keep in mind that confidential information is not limited to current R&D activity or proprietary manufacturing formulas or processes. It also includes customer data, business plans, terms and conditions in agreements with trading counterparts, employee personal data, future targets, and many other items that could be of use to your competitors or counterparts.

Following are some additional key points to keep in mind:

1. Follow strict exit procedures

It's crucial to have a definite plan in place for handling personnel departures. Specific template documents should be prepared for handling ordinary resignations, layoffs, terminations

for poor performance, and terminations for serious misconduct, respectively. Exit procedures should always take into account the confidential information that the employee may have in his or her possession, providing a timeline for the return of such information and the closing off of the employee's access to confidential information in the company's systems.

Timing of the shutdown of access to email and company networks should reflect the nature of the departure. In cases involving immediate termination for misconduct, the company should take special care not to allow the employee to have access to systems where they may attempt to download or erase files, or otherwise disrupt company activity.

Depending on the situation, many companies will have corporate security either present or ready to step in if needed during a termination. In some cases, corporate security may take a lead role in certain exit procedures, such as retrieving company key-cards, computers, smart-phones, car keys, etc. Personal effects in the individual's office may be packed up separately and couriered to the employee's home so as to avoid an emotional scene or gawking employees.

The plan used in a for-cause termination should be aimed at maximum efficiency and smoothness so as to help preserve the dignity of all parties concerned. An employee who is terminated without public humiliation or embarrassment is less likely to seek creative means to try to "get even" with the former employer, and more likely to move on to a new career chapter.

2. Keep basic psychology in mind

A psychological basis nearly always underlies misbehavior such as the theft or misappropriation of trade secrets. Often acting under stress or pressure, the employee taking the confidential information or sharing it with others views the risk/reward ratio as being in their favor.

The motivation may even be love. Some years back we had a case in which a man and woman (married but not to each other) were having an affair while working for companies that did business with each other. The client's IT team figured out that one of the company's employees was using his personal web-based email account to send future product plans to his lover, who worked for a distributor that also handled some competing products. He didn't benefit financially, and subsequent investigation found that no information had leaked through to competitors. But for a few months he was able to make his lover appear to be extremely knowledgeable within her company about a key supplier's future business and product plans.

In another case, one of hostile termination, a senior manager was recalled from overseas and informed of his impending termination on the first day of a two-day effort to negotiate a smooth departure. At the close of the first day's negotiations, the company had not yet shut off the manager's access to the company's email and database systems. Computer forensics examination would later confirm that the manager got up in the middle of the night, apparently unable to sleep, and spent the rest of the night downloading – and attempting to download – vast amounts of emails and data. Why? Jetlagged, stressed managers in the midst of a termination don't always think straight, so don't expect that they will necessarily make the right decisions. Follow an orderly procedure to remove access to company information immediately.

Especially in cases involving termination of IT staff, it's vital not to give advance notice that would give them a chance to get swift and disastrous revenge. Client situations have included:

- A magazine-publishing company that discovered that every article and photograph for an upcoming 48-page issue had been completely deleted from their servers just a week before going to print;
- A public relations agency whose IT guy's last 24 hours were spent loading every computer (including servers that had not even been connected to monitors) with pirated versions of software. The ex-employee then reported the supposed infringements to the makers of the legitimate software;
- An employee who registered domain names very similar to his employer's URL under his own name. After termination, he then set them so that anyone inadvertently landing on those addresses would be automatically forwarded to the website of his ex-employer's main competitor.

3. Be tough – to keep the case short

Once the evidence has been compiled that an employee has taken confidential company information, a variety of opinions may be expressed among the company's executives and their legal advisers as to the best way forward. But it is extremely important to adopt a firm position quickly and to maintain it, or else the case may drag on for a long time, becoming a financial and emotional burden.

The company's management may wish to believe that the recently terminated manager simply copied 30GB of the company's data out of a misplaced desire to keep a "souvenir" or "record" of his or her work. But from a legal perspective, it's essential to act quickly to stop that data from reaching a competitor or an upstream or downstream counterpart. Trade-secrets cases are difficult. They require focus and discipline in order to get swift action from the courts and, if possible, to scare the party who took the data into returning or deleting it.

In these cases, too many cooks can spoil the broth. In a case some years ago, we watched a company essentially "average" the advice received from several retained law firms, coming up with a case approach that was never strong and never decisive. Going back and forth between "hard" and "soft" approaches doesn't deliver any strategic or tactical advantage to your company and only adds to the cost in legal fees. To solve the problem, we had to persuade the client to "reset" the case with a strong commitment to use the solid options available under Taiwan's criminal laws. That decision swiftly brought the other side to the negotiation table.

Think of the challenge as being like using an axe to cut down a tree. You'll accomplish nothing if you just give a couple of gentle taps against the trunk and hope for the best. In a trade-secrets case, you must move quickly to ensure the other side knows that all hell will break loose if they don't hand back the stolen information. The likelihood of getting effective court action or a swift settlement increases immensely if the other side knows you're ready to go the distance. Also, the likelihood of getting longer-term compliance from the rest of your employees goes way up if they know that you're ready to be tough on trade-secrets theft.

4. Think flexibly

Is there a cross-border aspect to the theft or misappropriation that might bring additional legal jurisdictions into the picture? In many cases in our experience, important conduct related to the misdeed occurred offshore, sometimes during trips to the United States where the very tough Economic Espionage Act is in force. A former employee may find that his or her future employment options are greatly reduced if they can't travel internationally or return home without facing possible arrest at the airport.

5. Don't overdo it

In cases we've worked on from the employee perspective, we've also seen companies make the opposite mistake – pursuing spurious charges of trade-secret theft where no basis actually existed. Companies that rush to take drastic action against employees departing in good faith can find themselves opened up to substantial liability. Given the tough criminal sanctions for violations of Taiwan's Personal Information Protection Act (PIPA), it is absolutely essential that companies act responsibly in their effort to investigate employees.

In one extreme case, the departing employee voluntarily turned all of his personal computer drives over to corporate security for a final requested review to ensure that he was not taking away any company data. The drives included his only copy of many years of family photos, all his financial data including his tax returns, and vast amounts of other highly personal data. The former employer's security team then retained the data for months, copied and kept all the employee's drive contents (including the family photos and financial data) without the former employee's permission, and only later thought to ask the former employee for signed permissions. The company soon found it running into problems under Taiwan's PIPA for its unnecessary and unauthorized copying of highly private data.

The company could have saved itself considerable litigation costs if it had simply reviewed the employee's personal computer drives swiftly and returned them with no further copying or retention beyond the scope of the employee's consent. Good judgment must be used in evaluating which cases to pursue as well as the methods used to pursue them.

6. Bringing it together

A successful trade-secrets program in the workplace needs to create expectations among the employees – expectations about their own behavior as well as the company's determination to take strong countermeasures when necessary. Holding regular training sessions can be very useful for building a compliance environment, but they should be structured to ensure that the information imparted is understood and retained.

Once you've confirmed that solid evidence exists of a trade-secrets theft or disclosure, the company must take swift and decisive action to pursue the matter in order to increase the likelihood of getting the other side to back down. Any half-measures will be interpreted both by the courts and by the counterparties as demonstrating a lack of resolve and certitude. If your own investigations leave you with incomplete information about what's happened, consider getting official police resources involved so that a more intensive investigation can be pursued under the approval of the courts.

But if convincing evidence of trade-secrets theft is absent or if there are clear signs that the former employee is acting in good faith, the better course is to back off. A company should never take actions on its own or use private investigators in a way that could be deemed a violation of an individual's privacy rights, as serious penalties may result.

— John Eastwood is a senior partner heading Eiger's intellectual property and employment law practices and regularly works with clients on their Taiwan and Greater-China matters.