Losing Trade Secrets To Foreign Companies: How To Reduce The Risk

March 1, 2017 by James Pooley

During a recent seminar I was asked, “What can companies do to stop the loss of trade secrets to places like China?” The questioner seemed stressed and a bit angry, perhaps reflecting a certain frustration that there may not really be an answer. While I can understand the concern, and although there is no way to entirely eliminate information security risks when doing business overseas, we certainly can reduce them.

The modern commercial environment is inescapably digital and global. Long supply chains and open innovation strategies require sharing valuable information with actors in countries where legal protection systems are not robust. Companies increasingly employ foreign nationals, both in the U.S. and in installations abroad. And just like any other employees with knowledge of your secrets, they tend to move about.

The legal backdrop for all of this can seem confusing. If you look at the WTO standards for trade secret protection laid out in the 1995 TRIPS Agreement, they look pretty solid. (They also look familiar, since they were adapted from the Uniform Trade Secrets Act.) But the problem lies in enforcement. Bringing a trade secret claim requires access to proof, and civil law countries don’t provide discovery. So you need to perform your own investigation and then deal with the local authorities. We’ll look at some things you can do to improve your chances in litigation; but first let’s consider how to manage relationships to avoid problems in the first place.

Set a security strategy

First, you need to set a strategy for handling your most valuable data. Inform yourself about the places where you think you might have to expose that data; what cultural differences might influence the way that people there will respect your rights? Are there local laws and policies on employee rights that could affect the trustworthiness of the people who will have access? Some cultural practices, such as the acceptability of “trading favors” or the ability of friendships to trump business obligations, could alter your risk calculus. Note that we are dealing here with the classical “insider

threat” through which most critical information is lost. Whether the loss occurs through some electronic connection is not the point; the weak link is the personal actor.

And so in addition to the local cultural and business environment, your strategy has to consider the various relationships that will be implicated: collaborators, outsourcing partners, vendors, distributors and even customers can be vectors of information loss. If you intend to operate through a local subsidiary or establish your own local research facilities, then these too will become “endpoints” in your connected network. Finally, consider how these relationships will play out with other actors in other countries where you have operations.

As in any risk analysis, you have to be sufficiently informed about your environment so that you can make intelligent decisions about your appetite for risk. In this context, that means having a thorough understanding of what information assets you own, how quickly their value degrades, and what are the likely threats of loss. Understanding all of this will help inform the decisions you make about particular deal structures, or about how you package your secrets and where you send them.

Beware of local sharing requirements

Some governments require that, as a condition of entering their markets, you may have to license your relevant know-how or other intellectual property to a local partner. In its most benign form, these requirements are intended to provide a kind of “training” to local industries, to help them move up the value chain and become more productive. In a darker sense, they can also be simply a way of forcing technology transfer to favor domestic companies. Either way, you need to consider the risk of loss as a cost of entering, or staying in, that market.

Some foreign laws regulate contracts, including nondisclosure agreements, to impose time limits on confidentiality. This can provoke surprises when dealing with local licensees, so if the information is particularly valuable look carefully at these restrictions, and at competition laws that regulate issues like territory or use restrictions on dealing with your data.

Of course, some local partners can be very valuable in helping a business succeed, by applying their special knowledge or connections. And some

markets, such as China or India, are so huge that the risk of some information loss is deemed acceptable. The point is not to avoid doing business in these places because they are risky, but to consider carefully the nature of the risks so that you can make smart decisions.

Pick your partners carefully

Legal issues are only a part of the picture when considering foreign operations. Because trade secret protection fundamentally relies on trust, your first line of defense is the integrity of the people you will be dealing with. So employ a “know your partner” rule. Thoroughly investigate before establishing the relationship, and carefully monitor and manage it throughout. This applies to the usual external relations with collaboration or outsourcing partners, vendors, distributors and customers. It applies with special force to your local managers, who will have ongoing access at some level to inside information, and they should be subject to extensive background checks (as well as solid contracts and ongoing training and close supervision).

For each of your potential corporate partners ask: how well can I trust this company? What will it do to protect the secrets that I will disclose to it? Here, beware of the common but threadbare promise to protect your secrets with “the same level of care as is applied to its own.” Instead, get specific about exactly what they do to manage confidentiality. What sort of contract (confidentiality and noncompete) program do they have in place with their own employees? What is their training program for trade secret protection? Do they do background checks on their employees? What procedures are in place for physical and electronic security? How sophisticated and well-enforced is their own information security policy? Will they subcontract any of the work they are doing for you, and if so how do they protect against problems with the subcontractor, or with that company’s subcontractor? What has been the history of the company’s other commercial relationships? Does it have ties to the government?

Pay close attention to your contracts

In the U.S., contracts are important, but the law often will imply a confidential relationship, such as with employees or a long-standing supplier. The same is not true in most of the rest of the world, where secrets are often legally protected only by contract law. And the difference

is even greater when it comes to remedies and enforcement in case of a breach. When dealing with foreign actors with access to your information, what's in the contract is the most important factor.

Be very detailed about what information is to be protected, and how. This includes who is to get access and for what purposes. Also be specific about exactly what protection measures you expect for the facilities where your information will be kept, the IT systems that may be used with it, and procedures to be followed for return of materials at the end of a project. Where possible, require downstream agreements with all individuals and companies that may be given access (including noncompete provisions where allowed by local law), coupled with recordkeeping that will make monitoring compliance straightforward and easy. In fact, you may want to specify the content of these downstream confidentiality agreements to be sure that they name your company as the beneficiary of the secrecy obligation; in some countries, you may not be able to assert a claim if you are not named in the contract that binds that specific person or organization.

Expect to have to do more to manage and verify compliance when you are dealing with foreign relationships. Be sure that your partner is obliged to tell you when someone leaves the project team, and to take specific steps to follow up and ensure that confidentiality is respected by the departing employee. Require advance approval for any subcontracting. If you can get it, include an indemnity clause that puts the risk of loss on your partner in case there is a problem that happens through the people or companies they work with. Provide for regular audits and any other monitoring procedures that might be helpful.

Where possible, include specific and substantial penalties for any breach of confidentiality. Foreign courts may sometimes recognize these contract clauses and award much more than would have been available as normal damages. To ensure the most robust remedies, try to get the other side to agree to U.S. jurisdiction in the case of any dispute. (This may be most effective with companies that have existing relationships or assets in the U.S. that they want to protect.) Consider including an arbitration clause, which some foreign jurisdictions may be more likely to enforce than a general concession to U.S. jurisdiction. Arbitration has the advantage of privacy, and often can produce more effective remedies than you can get directly from a court.

Pay even closer attention to management

While contracts are important, the most detailed agreements are not a substitute for close, even obsessive, management. Don't take anything for granted, and follow up on every issue. Even though it will take up more time, you will be better informed, and your intense attention will serve a message that you are serious about protecting your rights. Encrypt and document all communications. Mark every document prominently as confidential, and create special procedures for handling particularly sensitive records.

Make information security a positive objective for your partner. Create incentives that are connected to good security outcomes. Encourage quick and full disclosures of any problem, including reports on what departing team members are doing. And provide (don't just require) continuous secrecy training to every person who has access to your data.

Maintain good local intelligence and connections

Before making any substantial investment in a foreign location, retain legal counsel who is familiar with the practical realities of the jurisdiction and has helpful connections with local law enforcement. It's not just about the content of the laws, but about how to get enforcement when there's a problem. Are there special restrictions on employee confidentiality or invention assignment agreements? Do employees have to be paid special compensation for their inventions? Are injunctions available? How much proof do you need to win? What damages can you expect to recover? What are the risks of pursuing a claim in litigation?

Divide and allocate access to secret information

One time-tested strategy for managing risks to your trade secret is never to let one person know all that's necessary to make it valuable. Brought to scale for large organizations, this divide-and-allocate approach can include:

- Sending only lower-value data into high-risk countries
- Separating steps in a production process to occur in different places

- Pre-mixing ingredients or preparing critical parts in a secure location
- Separating teams (and managers) according to various parts of a process
- Rotating managers

For example, automotive manufacturers going into developing countries have resisted doing their research and design work there. And when Sony increased its manufacturing in China, it clarified that some very important parts, such as the PlayStation game controller chip, would always be made in Japan, for security reasons. These strategies may not be sustainable in the long term, so be realistic about how long it will take for your current secrets to be compromised, so you can be working on making them more or less obsolete through your next generation technology.

Exercise care in traveling to foreign countries

Whether or not you establish facilities in foreign markets or enter into relationships that require sending your technology there, you or your colleagues will be "carriers" of your company's secrets whenever you travel. Here, apply equal doses of common sense and paranoia to avoid mistakes. Consider replacing your electronic gear – laptop and phone – for travel with stripped-down versions that contain only the applications and (encrypted) files you will need for this trip. Have them examined and "scrubbed" on your return, so that you can know whether there has been any attempted compromise and whether it is safe to transfer your updated files. While in the foreign country, assume that all internet traffic is watched and recorded. Always use encryption, and where possible use a Virtual Private Network (VPN) to connect to the internet. Avoid all public wireless networks. When in meetings, assume that conversations are being recorded.

Prepare for litigation

Trade secret litigation is hard, expensive and disruptive. Doing it in a foreign jurisdiction can be all of those things but worse. So first try to find a non-litigation solution to the problem. If that can't work, consider whether it might be possible to sue only in the U.S. If that is not an option, then consider this:

- Retain foreign counsel with a proven track record of success in these cases.
- Review your agreements and consider contract-based remedies.
- Before filing, do all that you can to investigate and gather hard evidence.
- Consider parallel actions in other jurisdictions (particularly the U.S.) to secure additional evidence or provide additional forms of relief.
- If a full scale injunction is unlikely or impossible, go for an early win with more limited relief, such as an order to preserve evidence.
- Demand compliance procedures, such as appointment of a monitor.
- Understanding that injunctions may be hard to get, focus on developing your damages claim.
- Carefully consider the pros and cons of a criminal complaint, and if you decide to go ahead, help the prosecutor plan for the most comprehensive seizure process by providing details of what should be found.