The **China Integrated** Analysis
December 2011

Protecting Know-How and Trade Secrets in China:
The role of a well organized management and internal IT

Contrarily to popular belief, China's legal system protects employer's proprietary knowledge, even if it is not patented or registered. However, like many Chinese laws, its Achilles heel is implementation. The anti-unfair competition law (promulgated end of 1993 and interpreted by the Supreme Court in December 2004) makes it a criminal offense for employees to transfer without authorization a company's trade secrets (proprietary confidential information). This grants companies, both foreign and Chinese, protection of their unregistered know-how.

Whilst the common understanding in the West is that "not knowing the law is not an excuse", China's approach towards it is more pragmatic, as reflected in the law itself that states that a trade secret is one for which "the obligee (…) has adopted secret-keeping measures". In other words, it is a Chinese version of the common understanding that if you leave your money in plain view and make it easy for anyone to take it, you share at least part of the responsibility for having it stolen.

Though different from what is practiced in Western countries, this Chinese concept can, to a certain extent, be understood when considering the socio-historical background of the country. Under the communist economy based on common ownership, there was no legal basis for the protection of proprietary know-how. Until not so long ago, you could find full copies of international textbooks in state-owned bookstores (albeit in special sections restricted to foreigners). Most importantly, enforcement with actual criminal condemnations really started only 7 years ago, after the Supreme Court ruling of 2004.

Under the circumstances, it would be perceived as rather harsh to suddenly start condemning those who might not realize that they are behaving illegally, and that especially since the state itself used to behave in exactly the same way. In present day China, this gap in discerning between what is right and wrong with regards to intellectual property can only be bridged through education. Rather than giving the burden of the education to the State only through punishment, the current legal concept pushes companies to contribute to the change of culture through prevention and, by requiring that companies clearly protect what they deem as important trade secrets.

Practically, what "protecting confidential information" means for an employer has several layers:

Assume that those you deal with do not know that intangible property is protected

First of all, while this seems obvious but is often forgotten, it is necessary to make it clear to all employees and stakeholders what is company proprietary information and what is not, i.e. clearly define what information has value to the company and what doesn't. The simplest way is to label all documents that are proprietary as such, for example as "Confidential", "Property of the Company", and then evidently also in Chinese since most local staff do not speak English.

Furthermore, clear non-disclosure clauses must be included in the employment manual, defining what exactly proprietary company information is, and that it is a crime to transfer it without prior authorization or use it for the benefit of others than the company. Management takes a giant step

toward a safe IP environment when it creates a culture in which every employee knows more than just the principles, and is permanently reminded of the rigors of protecting intellectual property.

In addition, confidential information must not be left available to everyone in the company, but provided only on a need to know basis and for the duration of time it is needed by the employees who receive it. This is also valid for suppliers: disaggregation of knowledge through organizational and physical separation of activities and vendors also minimizes the risk of critical losses.

This essentially means that confidential information must be treated like any asset of the company. Taking money as an example, if a supplier or an employee receives company assets (like cash for expenses) he or she acknowledges receipt of the money and has the obligation to return it or return proof that it has been used, according to company rules and instructions. The same needs to be applied to valuable trade secrets.

Make use of all available provisions

There are two elements provided by the law in terms of employee management that we feel are under-utilized. These are the possibility to have a non-competition clause for after the employees have left the company, along with the option of having a notice period longer than one month for know-how intensive companies and where employees have signed a confidentiality agreement. Both provisions when used properly allow to restrict the transfer of know-how and to ensure better internal transfer of knowledge when a key employee leaves.

Besides, while it is reasonably easy to gather evidence of an employee breaking confidentiality rules when working in a well managed environment, it becomes much more difficult once the employee has left the company. As a result, exit procedures in terms of returning information (including potentially stored on mobile phones) and legal confirmations at the end of an employment are critical and often underestimated.

The above legally-minded aspects are not meant to minimize the importance of staff retention strategies. They certainly play the most important role for the protection of IP and for the company productivity. However, a good communication and well-defined working environment, including in terms of know-how protection, do reduce the possibility of misunderstandings with employees and eventually provides them professional training.

Suppliers & distributors management is critical too

It is also important not to neglect the stakeholders other than the employees of a company. The above principles need naturally also to be applied to sub-contractors and suppliers who are important sources of know-how loss. Among others, the internal management of its employees by a supplier is often neglected while doing qualification audits. Staff of suppliers can leak information too. To some extent, distributors, agents and possibly clients also need to be taken into consideration. Particularly, staff of distributors often set-up their own businesses and become distributors of competitors, or even team up with other producers to make outright copies.

The Role of IT

While the above guidelines can realistically be applied in operational processes, today's digital world generates considerable practical difficulties, resulting in strong pressure and high requirements on companies' IT systems. Indeed, all a company's trade secrets are almost unavoidably stored electronically.

Detailing all steps that need and can be taken to support know-how protection with IT systems is not practical, essentially because the actions to be taken depend a lot on the company circumstances and the level of IT security that makes sense for each individual business.

At least, however, confidential information should be centralized on a server and access restricted to those who need the information. Access to critical data (like clients or blueprints databases) can be ensured by preventing the download of files to local computers in reasonably easy ways.

To identify unauthorized transfers, if any are suspected to have happened, a log and copy of all emails should be kept on the server. Other ways to transfer information (such as USB ports) need to be disabled on desktop computers, and laptops should only be cleared for storing public information and for read-only access. This can be implemented relatively easily also in small companies.

Naturally, the system must be well protected against hacking, therefore preventing conflicting situations where an employee or supplier who misused information could claim that such information was leaked through the hacking of her or his account or the company system. Minimal protection against hacking is a good firewall and enforcing that users regularly change their computer and email passwords.

We hope that the above can be of support to your operations. For more information on IP protection for companies in China, or for IT security measures do not hesitate to contact n.musy@ch-ina.com.

China Integrated

China Integrated is designed to facilitate the long-term, superior success of its clients in China.

With 20 years experience and comprehensive in-house expertise in research, legal, recruitment, tax, finance, IT/ERP & public relations, China Integrated is specialized in establishing or acquiring successful businesses and managing the back offices of its clients.

Through decades of professional experience and hands-on experience in IT system set-ups, HR concepts and stakeholders contracts, **China Integrated is in a particularly strong position to optimize know-how and IP protection** within a company by providing **integrated solutions encompassing all crucial HR, IT and legal related aspects.**

China Integrated has offices in Shanghai, Beijing, Hong Kong and Mongolia.

To receive our studies: “The China HR Paradox”, “Behind the China Kaleidoscope” and “2010 Doing Business in China: A Survey of European Companies” in cooperation with CEIBS, kindly see the Publications section of www.ch-ina.com.

Engineering your Success