Daily News & Analysis

Saturday, September 12, 2009 3:11:00 AM

How to guard your trade secrets from departing employees

DNA

The onset of the global recession led to the downsizing phase. This phase has indeed been a learning experience for employers, especially in sectors such as technology, outsourcing, media, telecom, pharma, etc, which ended up facing unprecedented issues from outgoing employees – including leaking of sensitive or proprietary information, ownership and assignment of intellectual property, theft of company property, etc. This article provides certain pointers for mitigating the risks and the legal recourse available in case of any breach.

Exit interviews

While on the one hand, employees may not even be aware of the confidential information (CI) in their possession, there have been instances of departing employees engaging in theft or destruction of sensitive data with an intention of harming the employer's interests. With disgruntled employees posting sensitive data on public blogs and even social media, employers have much more to deal with to ensure that CI does not get leaked. In most cases, the processes followed by the employer during an employee's exit (which at times are limited to a discussion and exchange of basic documentation) are in no way comparable to the detailed due diligence and processes adopted during the recruitment phase. Since Indian law does not prevent an employee from joining a competitor, it becomes all the more critical for organisations to conceptualise, document and implement a formal exit process to ensure there is no loss/misuse of CI and intellectual property (IP).

During the exit interview, in addition to return of company property, the departing employee should be reminded of his post-employment obligations including non-disclosure of CI and trade secrets, non-solicitation of employees and customers, etc. That apart, all CI held by the employee should be listed out in writing and he should be made to acknowledge such information, in order to enable the employer to produce documentation evidencing the employee's knowledge and possession of CI in case of court proceedings. If necessary, additional documents may be signed during the exit interview reaffirming the employee's continuing obligations.

Ownership/assignment of IP

As per the Copyright Act, 1957, unless contractually agreed, copyright created by an employee under a contract of service is automatically owned by the employer. However, similar provisions do not exist in other IP laws (especially the law on patents). Therefore, it becomes imperative that contracts with employees specifically include provisions for assignment of IP to the employer. If IP assignment agreements are not executed at the time of joining, these should be made part of the exit documentation, assuming the employee was involved in developing IP.

Monitoring and/or blocking employee's access

During notice period, the employer should take stock of company information containing CI or IP in the employee's possession or otherwise accessible to him. Further, monitoring the movement of information as well as data loss from locations where information is stored and blocking the USB ports/CD and floppy drives, may be advisable. Keeping a tab on the departing employee's emails (both official and personal, while using company's systems) helps mitigate potential violation or misuse of CI. A documented policy giving the company necessary monitoring rights is helpful.

Legal hold

A legal hold requires a company to preserve certain documents/information when legal proceedings in its connection are ongoing or reasonably anticipated. This concept, prevalent in some of the developed countries (for example, US and Canada), is not yet recognised in India. However, there may be situations where only the departing employees are aware where critical information is stored. Employers would do well to take stock of such information prior to the employees leaving, to avoid any complications in future with respect to the legal matters.

Legal recourse

In spite of adopting some of these practices to mitigate potential exposure in terms of disclosure, misuse or destruction of CI and IP, employers would also be relieved to note that there is sufficient protection available to them under law, in addition to

any contractual arrangements. Theft or misappropriation of company property, tangible or intangible, is considered a criminal offence.
The Indian Penal Code (1860) defines theft as "…to take dishonestly any moveable property out of the possession of any person…" 'Moveable property' has been defined to include "corporeal property of any description". Hence, if any data or information belonging to the company, stored in any tangible device is stolen by the employee, it could fall within the ambit of the above provision, leading to imprisonment up to three years and/or fine.
The Information Technology Act (2000) provides that if data is transferred electronically without the permission of the owner of any computer or computer system or computer network, liability may arise under its provisions. The penalty could be up to Rs 1 crore.

Moreover, committing acts which cause harm or damage to the employer entitles him to seek interim remedies against the employee and Indian courts, recognising the importance of protecting CI and IP, have been granting injunctions or interim relief fairly quickly.
While court proceedings are never desirous, employers should not take any such situations lightly. Quick and severe action against any employee for violation or misuse also helps create a psychological impact on other employees of the possible risk that they may face.

While the reviving economy may slow down the downsizing process, HR departments are better off putting in place the systems for protection of CI and IP in possession of departing employees. Before the golden handshake, it's time to pull up the sleeves!

Nishith Desai Associates is a Mumbai based international tax and legal counseling firm. The views are personal