Insider Threats: Protecting Against Rogue Employees

Most espionage is committed by insiders and arises from employees intentionally using or exceeding authorized access to company assets.

BY ALEXANDER MAY

Employees are typically a company's greatest resource but can also be the greatest source of legal compliance risk. Many companies go to great expense to protect their business, assets and secrets. While company firewalls may keep outsiders out, they do little to prevent insiders from exporting company secrets, exploiting corporate opportunities and self dealing.

An insider can be anyone with authorized access to a company's systems beyond that of the general public. It is now generally accepted that most espionage is committed by insiders and arises from employees intentionally using or exceeding authorized access to company assets.

Many companies in China fail to do all they can to protect themselves. We highly recommend a very tight contractual framework as a foundation. A broad but tailored employee handbook, tightly drafted employment agreements, comprehensive non-disclosure agreements and well crafted non-competition agreements are a starting point and should form an integral component of an overall internal risk management strategy.

"[…] over 50 percent of insiders who steal company information steal at least some of the information within 30 days of their termination and companies regularly fail to detect IP theft by insiders."

Internal threats can manifest themselves in various guises but they often come in the form of self dealing or theft. Self-dealing occurs when a director, corporate officer, manager or other fiduciary takes advantage of his/her position in a transaction and acts for his/her own interests rather than the interest of the company or the party to whom they have a duty. Self-dealing can involve the misappropriation or usurpation of corporate assets or opportunities. Self-dealing is a serious form of conflict of interest.

Many company assets can be stolen but theft is a critical issue in the case of intellectual property, which includes any sensitive or confidential information owned by a company that it would like to protect. Technology, together with IP, is generally the comparative advantage held by many companies in China, particularly western companies.

According to the Software Engineering Institute ("**SEI**") at Carnegie Mellon University, over 50 percent of insiders who steal company information steal at least some of the information within 30 days of their termination and companies regularly fail to detect IP theft by insiders.

All companies operating in China, both foreign and domestic, are at risk and should implement a robust infrastructure to manage insider threats. A good approach allows a company and its advisory team to:

- predict risk based on perceptions of variable circumstance and probabilities;

- pre-empt risk based on awareness of non-variable conditions and facts and predicted risks;
- quickly learn of and effectively respond to scenarios that could not be pre-empted or predicted; and
- mitigate damages when situations arise regardless of how they came about.

An approach to insider threat defense must be broad simply because of an insider's authorized physical and logical access to a company's systems and knowledge of the company itself. Insiders are aware of company vulnerabilities, with respect to both technology and business.

Because there is always a risk departing insiders might take valuable IP with them, the company must ensure all necessary agreements are in place (IP ownership, consent to monitoring, non-disclosure and non-compete at a minimum), critical IP is identified, key departing insiders are monitored and the necessary interdepartmental communication occurs. When an insider resigns, the company should increase its scrutiny of that employee's activities for at least 30 days prior to the insider's termination date. According to SEI, over 50 percent of insiders who steal company information misappropriate at least some of it within 30 days of termination or resignation.

Computer audit logs of employee online actions should be kept for at least 30 days so they may be scrutinized. Such logs must be protected from tampering by the insider and the person who monitors the logs must be trusted to report suspicious behavior found upon investigation. Actions taken before and upon employee termination are vital to ensuring IP is not compromised and the company preserves its legal options. Keeping audit logs for longer than 30 days may be useful for more in-depth investigation of suspicious behavior and for prosecution of any criminal activities.

A company must ensure its employees, as a condition of employment, consent to monitoring and agree upon the company's ownership of all critical IP. Data owners must identify and properly label their IP. HR must track insiders with access to IP so when the insider resigns HR can have IT staff or systems monitor that insider's online behavior for signs of suspicious IP exfiltration.

A company must be able to either block exfiltration or detect it and confront the employee. If the suspicious activity occurs prior to termination, an appropriate response must be formulated by management as part of the termination plan. If the insider has violated an agreement regarding the IP, the company may wish to pursue legal remedies pursuant to advice from legal counsel.

Non-Compete Agreements

A non-compete agreement ("**NCA**") is often an important tool to prevent senior employees from moving to competitors. There are a number of key issues with respect to the validity of NCAs. There must be adequate compensation and the scope of the NCA should be as clear as possible. Geographic scope is relevant to an NCA because different locales throughout China have different minimum requirements as to compensation for non-competition ranging from 20% to 60% of the employee's salary. Therefore, if an employer would like the NCA to provide nationwide coverage, the compensation would need to comport with the highest levels to be found in China to avoid challenge in areas with the highest compensation requirements. While the Labor Contract Law indicates the minimum non-compete compensation should not be less than the minimum local salary, different jurisdictions may impose more stringent requirements. In fact, a recent draft interpretation issued by the PRC Supreme People's Court indicates non-compete compensation should be 100% of an employee's prior month's salary. It is important to discuss these issues with experienced legal

professionals to develop a strategy and contractual terms that address a company's specific needs and relevant risks.

Confidential Information

Employees that violate company trade secret provisions can be subject to criminal prosecution. For example, under PRC Criminal Law, an employee that violates the sanctity of an employer's trade secrets causing a loss of exceeding RMB 500,000 could be subject to a prison term of up to 3 years. However, companies must make an effort to protect confidential information or trade secrets. Failure to adequately protect confidential information and keep it out of the public domain could result in a Chinese court finding such information was not confidential for the purpose of punishing employees that violate company confidentiality and trade secret policies. Pamir can collaborate with your organization to design protocols to protect your non-registrable, proprietary information in a way that satisfies the expectations of PRC courts.

Basic Protection Advice

- "Lock your doors," because computer passwords may not keep determined infiltrators from stealing.
- Encrypt sensitive computer files.
- Shred all paper documents before disposing of them externally.
- Don't discuss company secrets in unsecured environments.
- Don't assume your consultants are working on your behalf.
- A little paranoia can save a company from financial calamity and public embarrassment.

Insider Threat Protection

Audit and Strategy

Pamir's approach acts as both a sword and a shield. We audit a company's existing condition and future plans and recommend and make improvements where necessary. The key component of our approach, the shield, covers (among others):

HR Policy

- Advanced employee whistleblower policy with real incentives that does not undermine morale
- Comprehensive Employee Handbook
- Employee candidate due diligence and thorough background checks

Contracts

- Employment agreements
- Contractor agreements
- Vendor agreements
- Supply and manufacturing agreements
- Agreements with consultants
- Non-Disclosure Agreements
- Non-Compete Agreements

IT Policy[1]

- System and data access
- Saving and export policy
- Flash disk access
- Portable devices and smart phone policy
- External email access
- Company Cloud
- Company email screening

[1] Conducted together with our external security affiliates.

Post Violation Strategy

Ideally, we like to think the variety of efforts we undertake to preemptively protect our clients and mitigate the risk of rogue employees are a panacea. Our strategy is designed to discourage employees from betraying the trust and interest of their employers. However, no shield can completely guarantee complete coverage and sometimes the inducements of disloyalty prove too great. Our approach contemplates this reality so in the worst case scenario potential damages may be mitigated and the available recourse is maximized.

When a rogue employee is suspected or discovered, swift action must be taken. Let Pamir be your first response team to address key issues and avoid mistakes that could undermine any of your avenues of recourse. If you suspect an insider threat we will work with you to consider your suspicions and review your evidence. Where an employee has breached his/her non-compete obligations we can assist not only in pursuing the ex-employee but in some cases the new employer as well. We can help you develop a termination and/or pursuit strategy to either settle a matter outside the adjudication apparatus or ensure you can bring a strong case before a labor arbitration tribunal and the courts.

The Author

ALEXANDER MAY
Special Counsel
amay@pamirlaw.com
(T) +86-21-5256-9933
(F) +86-21-5256-9936

Taipei

7F, No. 214, Dunhua North Road,
Song Shan District
Taipei 10546, Taiwan
(P) +886-2-5588-1799
(F) +886-2-5588-1790

Shanghai

Suite 1801, Xingye Tower 168
Jiangning Rd. Jingan District
Shanghai 200041, China
(P) +86-21-5256-9933
(F) +86-21-5256-9930

Beijing

65 Xiaojingchang Hutong, Gulou
Dong Ave, Dongcheng District
Beijing 100009, China
(P) +86-10-6515-7574
(F) +86-10-6515-7574