Fraud Risks in Your China Business Operations

Commercial fraud and corruption are much more prevalent in China than what we are used to in the West, threatening the profitability and survival of foreign companies doing business here. Drawing on his experience in Asia, Peter Humphrey, the founder of ChinaWhys, highlights some firsthand examples where businesses have been undermined locally and offers his advice on how we can best protect ourselves and mitigate those risks.

Wrestling with Fraud Risks in Your China Business Operations

There are clear and ever-present dangers challenging UK companies who do not take adequate preventive measures. Companies with precious niche technologies are particularly vulnerable. Good fraud risk management can have a substantial impact on your bottom line. UK companies operating in China should strive to keep unethical elements out of their business. Otherwise, they can incur substantial losses.

The global supply chain shift of the past 25 years has pushed so much manufacturing and R&D into China, accompanied by increased outsourcing, localisation and technology transfers. It is all driven by commercial, cost-conscious logic but has changed the risk profile of companies because commercial fraud and corruption, according to Western and Chinese watchdogs, is at least four times more prevalent in China than it is in advanced industrial nations. Scholars at Beijing's Tsinghua University estimated that 16% of China's GDP is lost to fraud and corruption, compared with an estimated 4% fraud rate in the USA.

Very often, head office or a senior expat manager fails to show a hands-on stance - they do not visibly show they care about their operation; they are unable to reach out to all levels of employees; and they over-rely on a single point of reporting – usually a local hire with good English – to provide them with information about the operation. This person garners too much power over the whole business: language, connections to government, internal network, external social network, direct contact with suppliers, direct contact with distributors, and loyalty from other staff in the firm. In tandem, junior staff with an ethics complaint often have no way to talk to head office or senior expat managers even if they want to report it. This opens fertile ground for deception and fraud. Companies must tackle this risk with a good mix of policies and measures in the areas of HR, screening, training, checks and balances, internal controls, and the management of the expat-local relationship.

Faced by such challenges, more firms have been adopting ethics control programmes to pre-screen employees, vendors, distributors and prospective JV partners or acquisition targets. We have also seen more compliance audits. In short, due diligence, background vetting, robust responses to violations of internal controls or to unethical conduct, and early warning mechanisms to detect or avert fraud, are now being embraced in a more integrated fashion.

Greater efforts are visible in many companies to introduce or strengthen a Code of Conduct or Code of Ethics by tying it into employment contracts as well as contracts with suppliers and distributors, to outlaw unethical behaviour, especially collusive activity between staff and business counterparties. The more advanced companies are drilling the code into their workforce and associated firms through ethical awareness and compliance training.

Stories from The Trenches

1 One case that I handled involved a packaged consumer goods manufacturer where staff in almost every department colluded with a counterfeit syndicate to produce fake products and inject them back into the firm's distribution channels alongside genuine product. People in procurement, packaging, sales and distribution, in the warehouses and in trucking, and even in the R&D department, were in on the act. They even had a business plan with annual production and sales targets. The entire racket was masterminded by the firm's former HR manager. This explosive mix of faking, supplier-purchaser scams, distribution fraud, and technology theft forced the firm, at great cost, to restructure its China business, terminate agreements with crooked suppliers, staff, and distributors and end numerous partnerships. Needless to say, it was a painful episode.

2 Then take Anna, a purchasing manager at a multinational retail chain in China who found an imaginative way of making some extra money. Anna established a firm under her sister's name, concealing her involvement, and then disguised this firm further by giving it a very similar name and the same address as an official approved supplier of her employer, led by a man named Fred. That way, she effectively sneaked in this proxy firm through the back door and on to the multinational's list of approved suppliers. Fred, head of the official supplier whose company name and address Anna used to perform this confidence trick, was complicit – he bribed Anna in return for her approving Fred's supply of goods at inflated prices to the multinational, and as a bonus Fred also allowed Anna's firm to supply to the multinational by piggy-backing on his own firm. So Anna had it coming both ways: she received bribes from Fred, and enjoyed the lavish proceeds from the sales her own firm made by supplying to her own employer.

3 Another case involved a scientist working for a life sciences multinational in an R&D team that had developed an innovative cost-saving industrial process. The firm had patents on the technology and expected to make hundreds of millions of dollars in profits by building plants using this technology. Indeed the first contract had been signed. The scientist suddenly resigned and was later found to have copied all the related files from the IT system on to CDs and was working with companies in China to build a business around this stolen technology.

We have to conclude that in most such cases the victim companies have neglected best practices, basic business controls and measures to reduce the risk of such a disaster happening, and they reacted too slowly to first signs that the problem existed.

Safety Tips

To prevent fraud, companies should have a robust and comprehensive program of anti-fraud measures in place. Here are a few suggestions:

- Background screening of staff, vendors, distributors, resellers etc
- Due diligence beyond the balance sheet – check the people
- Strengthen internal controls & monitoring
- Check compliance with internal procedures
- Educate your staff in local and international laws, ensure compliance
- Conduct internal audits, fraud risk assessments, process reviews
- Impose a Code of Ethics (COE) and bind it into all contractual relationships
- Hold ethics awareness training to drill the COE into staff and partners
- Use a whistle-blowing hotline and treat ethics complaints seriously
- Introduce checks and balances to prevent cross-departmental collusion
- Show a hands-on management style
- Use clear and visible deterrents, punish the violators
- Be vigilant against alternative loyalties centering on cliques
- Cultural differences must be well managed, avoid the "them and us" syndrome

[Article released in January 2013]

Author: **Peter Humphrey**, founder and Managing Director, ChinaWhys
ChinaWhys is an advisory firm promoting business ethics and transparency.