

# R&D Stampede into China Increases Need for Risk Management



Peter Humphrey  
Managing Director  
ChinaWhys

Hardly a day goes by these days without another big multinational announcing that it is setting up a Research and Development Centre in mainland China. In many cases, companies are moving their entire global R&D from home turf to China. In recent months we have seen chemical companies such as DSM from Holland and Ciba from Switzerland, pharmaceutical companies such as Novartis, Roche, and Pfizer; high-tech firms such as Siemens, IBM, Honeywell, Schneider Electric, Infosys; or aircraft makers such as Airbus and Italy's Agusta, shifting R&D operations to China. It appears to be a veritable stampede.

Corporations believe that there are undeniable cost-benefits to be had from making this move. It is much cheaper to hire a Ph.D. in China than it is in Europe or America, the logic goes. Moreover, China is granting attractive tax and duty concessions and other favours to multinationals to encourage them to make this R&D shift. There are also strong arguments heard in favour of integrating R&D more closely with major manufacturing centres on the Chinese mainland, where multinationals are increasingly making all their goods both for domestic markets and the world.

By one estimate, more than USD 4bn has been in R&D centres in China by companies from Japan, the US, Europe, Taiwan, and Hong Kong. There are now close to 700 corporate R&D centres in the country, mostly located around Beijing, Shanghai, and the Pearl River delta. Perhaps this all makes good commercial sense, but people in the risk management business have seen some situations unfold in China that suggest corporations need to take stronger measures to protect their intellectual assets from theft and abuse. China is after all the world's greatest centre of counterfeiting, patent abuse and other intellectual property violations. And while Chinese laws look good on paper, enforcement and justice are often not forthcoming when companies fall victim to a major IP crime.

We recently encountered the case of a large chemical firm that had made major steps in the development of nanotechnology, the new frontier in technological development for mankind as a whole. A Chinese R&D scientist who had

worked for the company for some years abruptly resigned and when the in-house IT engineers examine his computer, they discovered that for the last year the employee had been systematically downloading all the files from the firm's R&D registry on to compact discs and he had evidently taken the whole lot with him. It was then discovered he had developed tight ties with several of the company's distributors and suppliers in mainland China and was busy forming a new business with them to absorb and utilise the technology that he had stolen.

Another recent case involved a Chinese scientist who was working for a big life sciences multinational in an R&D team that had developed an innovative and cost-saving industrial process. The firm had taken out patents on the technology and was expecting to make hundreds of millions of dollars in profits by building plants using these scientific advances. Indeed the first contract had been signed. The scientist suddenly tendered his resignation and was later found to have copied all the related files from the IT system on to compact discs and was working with companies in China to build a business around this stolen technology.

In both these cases, the victim companies had to launch into costly legal and investigative efforts to bring the thieves to justice. Neither company was able to obtain full closure on the case. There was a lack of understanding or sympathy on the part of Chinese enforcement agencies and judicial authorities. Basically the crooks got away with their crime.

## Preventative Risk Management

So in a situation where it appears very difficult to win justice, corporations must learn how to identify and manage the risks and reduce their potential losses. Preventative risk management is essential in this environment. In our experience a number of measures are vital ingredients in the approach to mitigating the threats to your technology.

- High security standards: A detailed security policy must be put in place. In implementing the rules, lead by example. Engage professional security staff. Make sure all secu-

rity contractors are properly vetted. Have security audits conducted by professionals at least half yearly. Reinforce the system with regular security awareness training for staff and senior management.

- **Enforce strict IT security:** A strict IT regime policy must be introduced. Staff must be made properly aware of this policy. Violators must be caught and punished. State-of-the-art firewalls and data protection should be used. Establish well-known prohibitions such as a ban on password sharing, ban the use of email for personal purposes, the use of Internet for non-company activity, the copying of files or the emailing of files to home, the use of portable media capable of storing large amounts of data. Consider physically preventing the use of portable storage media. Consider restricting cell phone use in the workplace. Thorough vetting of IT personnel is essential. Engage reliable professionals to provide third party support and IT system security audits.
- **Training:** Arrange ethics awareness training for all staff and tie it in with a code of ethics. Provide fraud awareness training for key finance staff and managers. Provide security awareness training for staff and managers at various levels. Introduce contingency planning and crisis management training to deal with emergencies.
- **Reference checks:** At a bare minimum, companies should independently check all references provided by applicants and independently solicit written references from confirmed referees, even when assistance from executive search firms is available.
- **Personal background checks:** For senior staff, who handle precious intellectual assets, companies should go beyond references and probe a person's background. Is he who he says he is? Verify the past jobs he claims to have held. Establish the real reason why he left each job. Has he ever been involved in intellectual property disputes? Check with past employers and associates

on character, track record and integrity. Check whether he owns any companies.

- **Due diligence:** If you are teaming up with a local company for an R&D operation, conduct in-depth background checks. Where transparency is lacking, companies have patriarchal leadership structures, and where corporate governance is weak, due diligence on a partner or acquisition must go beyond the balance sheet. Numbers can lie. You must look at the people. Especially whether any of them have intimate ties with your other staff, or any past history of IPR violations or litigation.
- **Hiring restrictions:** Ban the hiring of relatives and conducting business with close relatives of staff and managers. Collusion between employees and their friends and relatives is the most common recurring factor in white collar crime cases in China.
- **Culture gap:** Multinationals must proactively bridge the language and culture gap. The gap itself is a risk, as it fosters an 'us and them' atmosphere, and produces temptations and opportunities for abuse. The multinational HQ and expatriate representatives must penetrate local culture, get to know their Chinese staff as individuals, and develop an understanding of the nuts and bolts of the business. Too many segregate themselves from 'the locals'. This alienates Chinese staff. A careful balance must be struck in the expatriate-local management mix. Staff-relations policies must encourage inter-cultural understanding.

### Best Practices

Ultimately, the lesson in white-collar cases in China business operations - and there is potentially one at every major multinational here - is that they could be prevented by using best practices. Managers must learn to identify, manage, and reduce the risks. It pays to provide resources for risk management from day one. Immediately installing strong controls and implementing them visibly will help prevent enormous potential costs and failures in the future. ■

### PROFILE

ChinaWhys is an independent risk management consultancy that promotes transparency and ethical practices and provides discreet risk mitigation solutions, investigation, consulting, and research services to corporations in matters of high sensitivity across Greater China and Asia. Its founder Peter Humphrey has dealt with China and nations with similar systems for three decades. He is an expert on China fraud and supply chain risks, has resolved critical problems for many top multinationals and works closely with leading corporations and law firms. He has helped neutralise a counterfeit-and-fraud syndicate that hijacked the business of a global consumer goods maker, eliminated fraud from the procurement of a leading retail chain, unwound fraudulent JV deals for a global appliances manufacturer, and orchestrated the resolution of a child kidnapping in China. Peter is also a member of Rotary International and is engaged in charitable projects benefiting underprivileged children in the Chinese community.

### CONTACT

**Peter Humphrey** | Managing Director | ChinaWhys Co. Ltd.

35-107 CITIC Square | 1168 Nanjing West Road | Shanghai 200041 | China | Tel: +86-21-5111 9194 | Fax: +86-21-5252 4616  
Mob: +86-1376 430 3928 | E-mail: peter.humphrey@chinawhys.com | www.chinawhys.com