The Economist

Corporate espionage

Who needs cyber-spying?

Old-fashioned theft is still the biggest problem for foreign companies in China

Feb 23rd 2013 | SHANGHAI |From the print edition

ON JANUARY 5th, in a night raid, a gang of criminals broke into a factory near Shanghai owned by Mercury Cable, an American manufacturer of high-voltage equipment. The thieves took not only raw materials but machinery from production lines as well.

Who was responsible? Todd Harris, the firm's American boss, blames a gang led by a former manager at the plant. He claims local police have refused to take action despite repeated complaints, and that former employees and local officials are colluding to "set up a Chinese company making knock-offs." Cybercrime may be sexier, but the hard reality for companies doing business in China is that old-fashioned skulduggery remains a bigger threat.

The Mercury saga is a common tale. A foreign businessman comes to China with dollar signs in his eyes, struggles initially, then finds promising local managers who speak English, and he hands over the keys to his factory. He visits occasionally to woo local politicians over endless banquets. The business at last booms, until one day everything suddenly falls apart. Typically, the foreign firm loses vital intellectual property (IP) and assets, and cannot find any local remedy.

Boots on the ground

"The easiest way to get intellectual property from a firm is by buying or renting an employee inside it," says Kent Kedl of Control Risks, a consultancy. He frequently encounters cases in China of Western clients losing technology, sensitive sales data or, as with Mercury Cable, entire production lines. Some criminal tribes operate inside the target firm and misappropriate its resources, while others use purloined property and know-how to start rival businesses after (or even before) leaving the firm.

The most dangerous local thieves are "PhD pirates", says Peter Humphrey of ChinaWhys, a fraud-investigation consultancy. Such engineers and scientists may work quietly for years inside multinationals, especially in research-intensive industries like pharmaceuticals and chemicals, before striking. Mr Humphrey says there is a lively market for stolen intellectual property in China, and insists that "the massive expansion of Chinese patents is based on dubious ownership".

What can companies in China do? Some Japanese firms allow only trusted employees from the home country to mix secret formulas. Other companies are rethinking the business-school mantra that senior managers must be localised rapidly in emerging markets since they know the markets best. The boss of a Western multinational which got burned in a local corruption scandal concluded that he did not know whom to trust in China, so he put foreign managers back in charge.

The chief technology officer of a Western chip-making giant says his firm has a research centre in China but “would never bring the crown jewels into the country.” He orders his team to smash (not wipe) laptops and mobile phones after visits. If the technology matters, “then don’t bring it to China as it will get stolen,” says Jay Hoenig of Hill & Associates, a consultancy.

Many companies are aware of the dangers, yet still fail to take enough precautions. One reason is naivety. It will not happen to me, think some. Another is that foreign bosses often do not speak Chinese, observes Mr Kedl, and are unaware of the local culture of “favour trading” that can lead employees to give away secrets. One other factor is pressure to show results quickly. Managers deploy the best technology in the country, knowing it is at risk, because they must do well in order to advance their career.

Problems also come from the Chinese requirement that foreign firms in “strategic” sectors transfer certain technologies to local partners. The snag is that it is hard to set up a factory in which some secrets are to be shared but not others.

A more nuanced explanation is that heavy-handed IP controls of the sort advocated by security experts run counter to the culture of collaboration and trust that innovative companies cherish. At such firms, executives know their technologies will leak out one way or another. “Staying out of China in hope of keeping our IP safe is obviously not an option,” says John Rice, vice-chairman of GE, a multinational conglomerate. It can be stolen anywhere in the world through cyber-hacking, he adds. At such firms, the best way of keeping ahead is by quickly inventing the next generation of technology.

See also:

http://www.economist.com/news/china/21572228-evidence-mounting-chinas-government-sponsoring-cybertheft-western-corporate?frsc=dg%7Ca

http://www.economist.com/news/leaders/21572200-if-china-wants-respect-abroad-it-must-rein-its-hackers-getting-ugly?frsc=dg%7Ca