Financial Times (London,England)

March 14, 2003 Friday
London Edition 1

SECTION: COMPANIES & FINANCE THE AMERICAS ; Pg. 27

LENGTH: 775 words

HEADLINE: Silicon Valley stars in its own spy thriller: Trade secret theft is big business, write Scott Morrison and Richard McGregor

BYLINE: By RICHARD MCGREGOR and SCOTT MORRISON

BODY:

3DGeo Development, Silicon Valley company, had its first scrape with trade secret theft several years ago when a visiting PetroChina employee was collared trying to hack into its computer system. Then last year a second visiting PetroChina employee was caught trying to download 3DGeo's source code, the foundation for its proprietary seismic imaging software.

The US company dealt with the first case internally but the second suspect did not get off so easily: he was arrested while trying to flee the US.

Such stories are increasingly common in Silicon Valley, home of the US high-technology industry. The region has seen a "significant and steady increase" in the number of complaints about trade secret thefts and **economic espionage** over the past three years, according to Ross Nadel, assistant US attorney in northern California.

A recent spate of cases involving Chinese nationals and companies has further raised concerns about China's efforts to obtain US technology for commercial and military use.

"It's an open secret that the Chinese covet everything," says a former partner at one Silicon Valley venture capital firm.

Such crimes often go unreported for a number of reasons. Companies may never learn of thefts, they may be worried about the effect of bad press on stock price, or about upsetting officials from the country involved or they could have concerns about revealing from where thefts occured. A recent survey by the American Society for Industrial Security and PwC estimated that Fortune 1,000 companies lost up to Dollars 59bn in 2001 due to the theft of intellectual property and proprietary trade secrets.

Donald Przybyla, supervising agent at the FBI's office in Palo Alto, California, estimates that 40 per cent of trade secret theft cases investigated by his unit involve foreign nationals or companies. At least 20 nations have tried to steal US trade secrets over the past five years, he said.

Most attention has focused on China, which has long had a reputation for ignoring Western concerns about intellectual property rights.

In an unprecedented move, officials granted US prosecutors permission to travel to China in March to interview 12 people who might be able to provide evidence against three Chinese accused of stealing trade secrets from Lucent Technologies, the US telecommunications equipment maker.

Prosecutors allege the defendants sold the technology to Datang, a rival controlled by a Chinese ministry, though US officials do not contend the company was complicit in the theft.

Cisco Systems, US networking equipment maker, in January filed a civil lawsuit claiming Chinese rival Huawei Technologies misappropriated and copied trade secrets to build cheap but sophisticated gear bearing a striking similarity to Cisco's products. Cisco has declined to pursue a criminal investigation.

Many Chinese companies are increasingly expected to act commercially and make a profit in a highly competitive business environment. That pressure to perform commercially is ample incentive to cut corners in acquiring technology.

Also, there is a strong sense in China that the US has used phony charges of espionage of different kinds, either for racial reasons or to impede China's progress.

Wang Xindong, an information technology commentator in Beijing, said that Cisco's lawsuit was mainly aiming to thwart Huawei's overseas expansion plans. "The bias of the US media case is obvious: they have judged Huawei 'guilty', though the case is not yet over," he says.

Companies such as Intel, the chip group, downplay the contention that economic espionage and trade secret theft is increasing. Rather, it is thought rising statistics simply indicate that companies are now more inclined to report espionage because federal authorities have started pursuing cases more aggressively.

Most commercial espionage cases involve insiders, usually disgruntled workers or employees who steal secrets in the hope of profiting. Smaller companies are more vulnerable because they have neither the experience nor the security.

But that does not make large companies immune. Last November, two Chinese were charged with economic espionage after being arrested at San Francisco airport with trade secrets allegedly stolen from Sun Microsystems, NEC, Trident Microsystems and Transmeta.

Meanwhile, increasing numbers of Silicon Valley's largest companies are looking to China and other developing countries to establish research operations, or to outsource manufacturing facilities.

One Beijing-based foreign security consultant said that, when it comes to corporate espionage in China, foreign companies remain "extremely naive".

LOAD-DATE: March 13, 2003