



ISSUE # 6 NOVEMBER 2009

CORPSEC TSCM NEWSLETTER

IN THIS ISSUE

- BEING WATCHFUL CAN HELP COMPANIES CATCH ESPIONAGE
- CORPORATE ESPIONAGE IS BIG GLOBAL BUSINESS
- GOTCHA! SOLOMON LEW SPYSOL SPY NETWORK EXPOSED FOR FIRST TIME

BEING WATCHFUL CAN HELP COMPANIES CATCH ESPIONAGE

By Edward Iwata, USA TODAY

It's impossible to thwart all economic espionage. But companies can make it harder for spies to rip off trade secrets. Here's what security and intelligence pros say to watch for:



EMPLOYEES LIVING LARGE. Stay alert for employees flashing cash and spending well beyond their means. It could mean they've been paid big bucks to pilfer your business secrets.

BACKGROUND CHECKS. Conduct thorough background searches on new hires, business vendors and joint-venture partners. Scrutinize their resumes and business and educational histories.

COMPUTER ACCESS. Limit computer access and passwords to key employees who need critical information. Change passwords often.

STRONG CYBERDEFENSE. Beef up computer networks and plug weak spots with the latest security software that detects cyber break-ins and monitors suspicious employees.

AUDITS. Conduct frequent security checks and audits. Many companies will set up security training and policies, but get complacent and fail to keep it up, Rudewicz says.

CORPORATE ESPIONAGE IS BIG GLOBAL BUSINESS

By GEOFF MORRELL

COMPANIES FEEL THE PINCH AS THIEVERY RISES

Corporate espionage used to be the stuff of children's books. Arthur Slugworth, a rival of the infamous Willy Wonka, is probably the best-known culprit. In Roald Dahl's "Willy Wonka and the Chocolate Factory," Slugworth tries to steal Wonka's secret recipes by bribing young visitors to the Oompa Loompa sweets maker.

Today corporate espionage is more cloak-and-dagger than chocolate-and-bubble-gum. It is big business, and with globalization, getting even bigger. "This goes on every day," says Ira Winkler, a top corporate security analyst. "Whether or not people want to admit it, it is very, very common."

BIG BUSINESS

Common and expensive. In his book "Spies Among Us: How to Stop the Spies, Terrorists, Hackers, and Criminals You Don't Even Know You Encounter Every Day," Winkler estimates American companies lose as much as \$300 billion a year to pirating, counterfeiting and other corporate theft.

Hacking into a company's computer system may be the most modern way to steal trade secrets, but experts say most thefts still occur the old fashioned way, by sneaking into a company's offices and making off with classified information. Inside jobs are another tried-and-true method. We just saw an example of that when several people were busted as they attempted to sell Coca-Cola secrets to rival cola giant, Pepsi.

SURVEILLANCE

The word *surveillance* comes from the French word for "watching over."

The word *surveillance* may be applied to observation from a distance by means of electronic equipment (such as CCTV cameras), or interception of electronically transmitted information (such as Internet traffic or phone calls). It may also refer to simple, relatively no- or low-technology methods such as human intelligence agents and postal interception.

Surveillance is very useful to governments and law enforcement to maintain social control, recognise and monitor threats, and prevent/investigate criminal activity. With the advancement of technologies such as high speed surveillance computers and biometrics software, governments now possess an unprecedented ability to monitor the activities of their subjects surveillance.

COUNTERSURVEILLANCE

Countersurveillance refers to measures undertaken to prevent surveillance, including covert surveillance. Countersurveillance may include electronic methods such as bug sweeping, the process of detecting surveillance devices, including covert listening devices and visual surveillance devices. More often than not, countersurveillance will employ a set of actions (countermeasures) that, when followed, reduce the risk of surveillance.

GLOBAL THIEVES

"Everybody does it," says Pat Choate, author of "Hot Property: The Stealing of Ideas in the Age of Globalization," and companies big and small fall victim to it.

While most theft involves American companies stealing from one another, more and more theft is being committed by companies overseas, especially in Russia, China and Taiwan. Of the 3,000 Chinese firms in the United States, Choate claims "a large number of them are engaged in piracy or stealing secrets and sending them back to China."

That's nothing new. Choate reminds us that in World War II, Japan built its Zero fighter plane from designs it had stolen from billionaire aviator Howard Hughes.

GOTCHA! SOLOMON LEW SPYSOL SPY NETWORK EXPOSED FOR FIRST TIME

Solomon Lew, secretive Melbourne billionaire, faces allegations of maintaining a private network of surveillance operatives throughout Melbourne.

Involving SpySol (or Spy Solutions) in South Melbourne and other shadowy companies associated with SpyMaster Gavin Warren, Lew is believed to monitor the activities of commercial rivals including photographic, electronic and physical monitoring.

Lew's spy network is believed to have monitored many prominent businesspeople over the years including the now jailed Rodney Adler (and his late father), Lawrence Gruzman QC (who investigated Yannon and the Etiket transactions) and several rival Jewish community figures in property development and retail. Game on.

WHAT'S YOUR COUNTERESPIONAGE STRATEGY?

The biggest security breaches in corporations these days are employees who have been laid off or who are about to get laid off.

When employees leave an organisation on their own terms, particularly in good times, many companies scramble to figure out what they had access to and what the value of that information would be to a competitor. There is a large body of case law in the technology industry involving theft of trade secrets, and globalization has added a new twist because laws in some countries are either unenforceable or nonexistent. But in a downturn where millions of workers are being cut, the scale of the problem grows by several orders of magnitude.



This is an information Newsletter and your feedback on any future contents would be greatly appreciated in order to keep it news worthy.

Corpsec Pty Limited is available to answer any questions or enquiries you might have on the subject of Technical Surveillance Counter Measures (TSCM)

If you do not wish to receive any further Newsletters please contact Nick Graves by email.

This publication is intended only to provide a summary and general overview on matters of interest. It is not intended to be comprehensive nor does it constitute legal advice.

We attempt to ensure that its content is current but we do not guarantee its currency. You should seek legal or other professional advice before acting or relying on any of its content.



Looking after your future
Listening to your needs

Nick Graves
Phone: +61 2 9267 0661
Email: ngraves@corpsec.biz