



ISSUE # 1 JUNE 2009

## CORPSEC TSCM NEWSLETTER

### IN THIS ISSUE

- ↳ A BRIEF HISTORY
- ↳ COMPROMISE CAN BE FATAL
- ↳ THE RISK OF CORPORATE ESPIONAGE

---

### A BRIEF HISTORY

The concept of eavesdropping is certainly nothing new. Electronic eavesdropping did not begin with Watergate; it was , by that time, at least 100 years old. It began when electricity was first used as a means of communications. During the civil War information was gathered by tapping telegraph wires. Indeed, countermeasures efforts were common by 1880 and 1890. Electric eavesdropping was considered a standard tool of both law enforcement agencies and private individuals. Remember, at that time it was not illegal. In fact, the technical art of eavesdropping has always been well in advance of the laws to protect against such action. There have been legislative efforts against technical surveillance since the year 1900 but they have not been very effective nor have they served as an adequate deterrent against this practice.

#### ARE MOBILE PHONES SAFE?

The interception and decoding of digital mobile telephones is becoming more commercially viable and therefore they should be considered a risk when being used for sensitive conversations. Mobile telephones can be reprogrammed or modified to act as listening devices, even when in "standby" mode, and therefore should never be turned on during sensitive meetings. It should also be remembered that most mobile phones have in built cameras with both single shot and movie capabilities. Where possible all mobile telephones should be left outside the meeting room.

## COMPROMISE CAN BE FATAL

Information is the lifeblood of today's organisation. Although it can be extremely difficult to estimate the value of information, it is widely accepted that the result of a compromise can be fatal. In a recent survey conducted by Price-Waterhouse-Coopers, ASIS International and the US Chamber of Commerce, (based upon Fortune 1000 business's) it found that 40 percent of all respondents had reported, known or suspected proprietary loss information.



The most commonly cited areas of risk by companies that reported an incident were; Research & Development (49%), Customer listed and related data (36%), and Financial data (27%) with an average cost to those companies of US\$404,000.00 (Research & Development) and US\$356,000.00 (Financial Data) per incident, per year. The total estimated loss to the US companies surveyed was estimated at between US\$53 billion and US\$59 billion, with an estimated overall intellectual proprietary loss (both foreign and domestic) in excess of US\$300 billion a year and rising.

Although these figures may seem excessively high, when compared to the sales of illegal eavesdropping equipment in the US at the same time (US\$888 million) it soon becomes evident that corporate espionage is of a major concern (especially when the US Chamber of Commerce estimates that of the \$888 million spent on 'Bugs', \$512 million worth of this equipment is currently believed to be installed in US Corporations).

Among these companies, the greatest impacts of proprietary information loss were increased legal fees and loss of revenue. For large companies (over \$15billion), loss of competitive advantage was the most serious problem. For financial firms, embarrassment was the biggest concern; and for high technology companies, the major issue was loss of competitive advantage.

Unfortunately no such figures are available for Australia. However, it would be naive to believe that similar activity (albeit on a smaller scale) does not occur here in Australia. Related research also suggests that the composition of corporate organisations' assets has changed (with the information asset becoming more predominant than tangible assets). This has risen from 38 percent to 62 percent in the last 6 years.

A prudent organisation will always take steps to reduce the risk to its products, assets and now more than ever its information.

## THE RISKS OF CORPORATE ESPIONAGE

### DID YOU KNOW?

Personal Digital Assistant (PDA) have become more popular with executives and other mobile staff and presents a new level of risk. Most PDA's now have mobile phones in built and also utilise other methods of wireless communications such as Bluetooth and Wireless LAN. Due to the limited Anti-Virus and software Firewalls available, these units are left vulnerable to an attack. Not only can data stored on these units be remotely accessed but the devices have the capability of becoming programmable listening devices with remote access and retrieval of conversations. These devices should be regularly checked for Viruses and Trojans and should not be taken into meetings.

Industrial espionage can generate an out-of-sight out of-mind attitude for companies that don't understand the value of intellectual properties or until confronted directly with the reality and cost of having information stolen. But Corporate Security Officers and Chief Information Officers (CIOs) around the world are seeing the need for greater diligence to prevent attacks, especially in economically challenging times. According to Merriam-Webster Dictionary, industrial espionage is "the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company." Unfortunately this definition seems to ignore espionage spawned from overzealous business competition, where one business may resort to espionage tactics (not necessarily illegal) to gain information providing an advantage over a competitor or to harm a competitor in some way. Regardless, information loss doesn't have to be espionage (illegal/

unethical) to be costly to the victim. Theft of corporate information occurs every day but is difficult to identify and track and often goes unreported. Disclosure of a breach acknowledges exposure to future loss and can be viewed as an embarrassment to the company and its stockholders, furthering financial loss (i.e. stock price affects from information loss acknowledgement).

**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)**



Looking after your future  
Listening to your needs

Nick Graves  
Phone: +61 2 9267 0661  
Email: [ngraves@corpsec.biz](mailto:ngraves@corpsec.biz)

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