



ISSUE # 3 AUGUST 2009

CORPSEC TSCM NEWSLETTER

IN THIS ISSUE

- ➔ **STORY FROM THE VAULT**
- ➔ **INDUSTRIAL ESPIONAGE 'REAL AND OUT THERE'**
- ➔ **THE SPY IN YOUR HAND**
- ➔ **EQUITABLE LIFE BOSS FINDS BUGGING DEVICE IN HIS FLAT**

STORY FROM THE VAULT

In 1946, Soviet school children presented a two foot wooden replica of the Great Seal of the United States to Ambassador Averell Harriman.

The Ambassador hung the seal in his office in Spaso House (Ambassador's residence). During George F. Kennan's ambassadorship in 1952, a routine security check discovered that the seal

contained a non electronic microwave device which could be stimulated from an outside radio signal.

Even after this bug was found this technology continued to be used by the Russian & Western intelligence services for another 4 to 5 years after.



May 26, 1960, Ambassador Henry Cabot Lodge, Jr. displays the Great Seal bug at the United Nations.

INDUSTRIAL ESPIONAGE 'REAL AND OUT THERE'

The revelation that Marks and Spencer is investigating an apparent attempt to spy on the mobile phone records of its boss Stuart Rose has brought industrial espionage into sharp and somewhat worrying focus.

By the very nature of the activity it is impossible to quantify, but experts are in agreement that the issue is real and growing. And the galloping pace of technology is making espionage, such as eavesdropping or theft, ever more of a potential problem for companies today.

Mobile phones and the internet simply provide the bad guys with a number of additional ways to get at a company's information, helped on by an ever more sophisticated and easily obtainable array of gadgets and tools with which to do their dirty work.

For example, an electronic bug can be enclosed in an apparently normal mobile phone battery, creating a listening device that is forever powered by the said power source and able to transmit the user's two-way conversation.

Listening in

Picture the scene: the company director hangs his coat up in the changing room before going off to begin his round of golf. The attacker then simply opens up the executive's mobile phone and switches the batteries.

REAL LIFE ESPIONAGE

In 2001 Procter and Gamble admitted spying on rival Unilever for information on its shampoos.

Boeing was punished by the US Air Force in 2003 for resorting to espionage in order to better its defence rival Lockheed Martin.

The director may never find out he was being bugged. After all, how many people know the file number on their mobile phone battery? Yet an unscrupulous rival can now listen to some of his most intimate business conversations.

"It is certain that the increased use of mobile phones and the internet means the potential to suffer from industrial espionage is bigger than ever.

Justin King (M.D C2i International) is in no doubt about the motivating factor behind the bugging trend: money.

"Information is vital when the markets are tight and people want to get an advantage. This is especially vital when in cases of mergers or hostile takeovers.

There are also a number of semi-legal firms providing spying services, Mr King added.

"These people are very easy to find, sadly it isn't hard," he said.

And in addition from simply protecting internet and phone systems, companies also need to keep an eye on their staff, be it full time workers or contract cleaners.

"I'm told the going rate to get a cleaner to steal something for you in London is £20," said Mr King. "We have had clients who have had a cleaner steal a vital document, or photograph it with a mobile phone, or even in one instance, simply copy it on one of the firm's photocopiers. You do not want to leave sensitive documents lying around.

Industrial espionage isn't just in films or TV shows.

THE SPY IN YOUR HAND



Speak up mate; I'm trying to record you here.

Don't talk: your cell phone may be eavesdropping. Thanks to recent developments in "spy phone" software, a do-it-yourself spook can now wirelessly transfer a wiretapping program to any mobile phone. The programs are inexpensive, and the transfer requires no special skill. The would-be spy needs to get his hands on your phone to press keys authorising the download, but it takes just a few minutes about the time needed to download a ringtone.

This new generation of user-friendly spy-phone software has become widely available in the last year and it confers stunning powers. The latest programs can silently turn on handset microphones even when no call is being made, allowing a spy to listen to voices in a room halfway around the world. Targets are none the wiser: neither call logs nor phone bills show records of the secretly transmitted data.

More than 200 companies sell spy-phone software online, at prices as low as \$50 (a few programs cost more than \$300). Vendors are loath to release sales figures. But some experts, private investigators and consultants in counter-wiretapping, computer-security software and telecommunications market research claim that a surprising number of people carry a mobile that has been compromised, usually by a spouse, lover, parent or co-worker. Many employees, experts say, hope to discover a supervisor's dishonest dealings and tip off the top boss anonymously. Max Maiellaro, head of Agata Christie Investigation, a private-investigation firm in Milan, estimates that 3 percent of mobiles in France and Germany are tapped, and about 5 percent or so in Greece, Italy, Romania and Spain. James Atkinson, a spy-phone expert at Granite Island Group, a security consultancy in Gloucester, Massachusetts, puts the number of tapped phones in the U.S. at 3 percent. (These approximations do not take into account government wiretapping.) Even if these numbers are inflated, clearly many otherwise law-abiding citizens are willing to break wiretapping laws.

EQUITABLE LIFE BOSS FINDS BUGGING DEVICE IN HIS FLAT

Bugged: Charles Thomson found listening equipment concealed in his apartment

The boss of one of the UK's largest financial institutions is at the centre of a security scare after a bugging device was found in his home.

Charles Thomson, chief executive of Equitable Life, called in police after discovering the listening equipment concealed in his luxury apartment in London.

Detectives are investigating how the device came to be in the Barbican flat, which Mr Thomson, 59, uses as a base during the working week. A security sweep has also been carried out at his £1million family home in Ayr, in Scotland, which he returns to most weekends.

Strathclyde Police say they have been handed a tape which is understood to contain a private conversation between Mr Thomson and his partner of five years, Verity Coutts.

DEFINITION OF TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM)

Simply defined, it is the systematic physical and electronic examination of a designated area by trained and qualified persons utilizing approved equipment and techniques in an effort to locate surreptitious listening devices, security hazards, or other means in which classified, sensitive or proprietary information could be intercepted or lost."

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

Back issues are available at www.corpsec.biz/TSCMOutlined.htm

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