



ISSUE # 5 OCTOBER 2009

## CORPSEC TSCM NEWSLETTER

### IN THIS ISSUE

- ↳ SOCIAL ENGINEERING
- ↳ NEW TECHNOLOGY - BUGGING IS AS EASY AS A WALK IN THE PARK
- ↳ LOW-COST GSM BUGS FLOOD EBAY
- ↳ PALACE ROOMS WERE REGULARLY SCANNED FOR LISTENING DEVICES

---

### SOCIAL ENGINEERING

Perhaps one of the most common ways for attackers to gain access to a network is by exploiting the trusting nature of your employees.

"You can have the best technical systems in place, but they're not effective if people aren't educated about the risks," says Mike Maddison, head of security and privacy services at Deloitte UK. A recent survey conducted by Deloitte found three-quarters of companies have not trained staff in the risks of information leakage and social engineering.

"It's vital that people understand, for example, that they shouldn't provide their password over the telephone, or that they recognise a phishing email," says Toralv Dirro, a security strategist with McAfee. "These sorts of messages are becoming increasingly sophisticated, and we're now seeing very personalised, targeted phishing emails that may even refer to projects that people work on, or members of their team."



## NEW TECHNOLOGY - BUGGING IS AS EASY AS A WALK IN THE PARK

It looks like a traditional phone adaptor but in fact it is a bugging device that will transmit calls. It remains a golden rule for spies of any persuasion that a walk in the park is still the safest environment for receiving secret information verbally from an agent.



Anything divulged inside a building or a private car is potentially open to an extraordinary array of electronic bugging devices or telephone intercept systems. Bugging is a fine art, and the technology has leapt forward in recent years.

The basic form of bug requires someone to listen in from several hundreds yards away, or to have a recording system hidden nearby that can store many hours of conversation.

However, the latest electronic listening device is known as the GSM bug. Michael Marks of Spymaster, a company that supplies surveillance equipment, told The Times: "With one of these new bugs, all you have to do is place it covertly under someone's desk. It's like a miniature cellular phone. You can ring it from thousands of miles away, it answers silently and you can listen in on conversations. The GSM bug could be in an office in London but the person listening to the conversations could be in Australia."

### LOW-COST GSM BUGS FLOOD EBAY

GSM bugs are simply tiny cell phones without keypads. Insert a SIM card, hide it, call its phone number, and eavesdrop from anywhere in the world. The lowest cost we've seen is 99 cents, plus \$21.99 shipping.

This is a major development in illegal electronic surveillance; amazing as it is scary. Anyone can be a high-tech spy for less than \$25.00. In addition to being packaged as tiny self-contained bugs, they are also being sold on Ebay (and many other Internet locations) hidden in every-day office items like power strips.



## PALACE ROOMS WERE REGULARLY SCANNED FOR LISTENING DEVICES

The Queen's rooms at Buckingham Palace were regularly swept for bugging devices, her former private secretary said yesterday. Lord Fellowes said the checks were ordered to "reassure" the Queen.

The high level of paranoia at the Palace in the 1990s was described at the inquest into the 1997 deaths of Princess Diana and Dodi Fayed.

In a letter to the Government, he said: "We would be much wiser as to the real risks of using mobile phones and whether it may be necessary to have all Royal residences comprehensively swept for bugging devices."



Asked whether the security services made checks on Buckingham Palace while he was working there between 1990 and 1999, he said: "The rooms in which business was conducted by the Queen and by her private secretaries were swept.

"I wouldn't say it was a constant preoccupation but we needed reassurance at regular intervals that there was no bugging going on."

The inquest has already heard that Diana feared she was under surveillance and called in specialists to sweep her apartments at Kensington Palace for bugs.

The High Court was reminded that the Squidgygate call was made on New Year's Eve 1989 between a landline at Sandringham and a portable car telephone in a rural area.

It said: "People who are intent on recording private telephone conversations between members of the Royal Family and their friends would be able to do so on a regular basis in a rural area by equipping a vehicle with a scanning receiver and tape recorder and positioning themselves within a few kilometres of the portable hand or car phone.

## CLEAN DESK POLICY

**CLEAN DESK POLICY - BY ANDREJ PROBST**



A clean desk policy is not just for the obsessive-compulsive. Have you ever thought of how much sensitive information may be left unattended on desk tops? A clean desk policy basically states that sensitive documents should be locked away if an employee leaves their office for an extended period. As with most policies, if you decide to implement a clean desk policy, you will need to exercise tact when you announce it, and patiently explain why clean desks contribute to security.

## QUOTE OF THE DAY

“Gentlemen do not read each other's mail “

**Henry L Stimson**  
**Former US secretary of state**

**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](mailto:ngraves@corpsec.biz)