

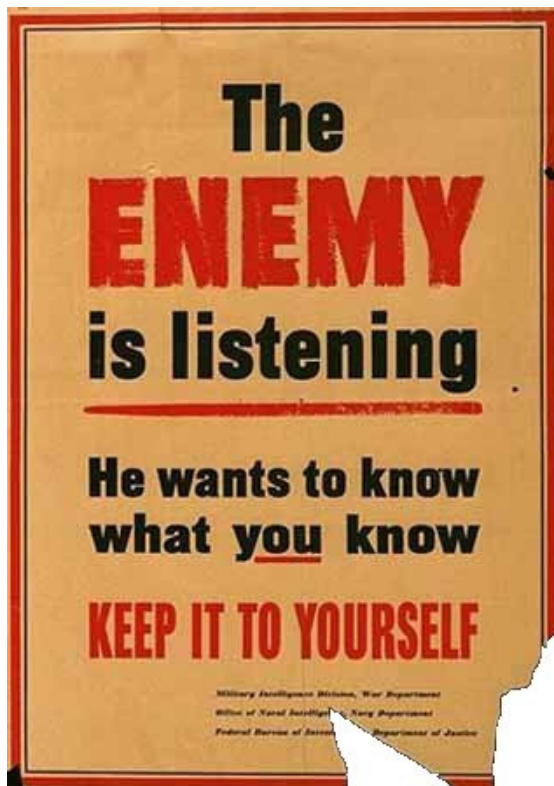


ISSUE # 4 SEPTEMBER 2009

## CORPSEC TSCM NEWSLETTER

### IN THIS ISSUE

- QUOTE OF THE DAY
- DEUTSCHE BANK FIRES TWO IN SPYING PROBE
- 'THIS GOES NO FURTHER...'
- WHAT'S BUGGING THE UNION LEADER?



### QUOTE OF THE DAY

"In essence, unless the company premises have been swept for bugs, there's no guarantee that somebody hasn't been listening in to your conversations regarding sensitive issues.

This could of course result in information regarding the company's products or services being leaked to competitors in the field.

Of course not many corporate managers like to acknowledge the fact that this could happen but the truth is; it can and does happen."

- Jacques Amaya, The Tech Edition

## DEUTSCHE BANK FIRES TWO IN SPYING PROBE

Two managers at the biggest German bank, Deutsche Bank, have left amid a probe into alleged spying. The head of security for the bank and its head of investor relations have been dismissed following an internal investigation into whether the company conducted surveillance on a board member and others. Prosecutors in Frankfurt, where the bank is based, are studying information provided by the public authority charged with the protection of personal data, based in nearby Darmstadt.

The cases concern alleged spying on supervisory board member Hermann-Josef Lamberti and outspoken shareholder Michael Bohndorf. Prosecutors can take two to three weeks before deciding whether to launch a formal investigation that could then lead to legal proceedings

Germany has been hit by several cases of corporate spying, at the telecommunications giant Deutsche Telekom, the national railway Deutsche Bahn and the discount retail chain Lidl. German privacy officials at the state and federal level routinely investigate reports of privacy violations by firms and government agencies. The privacy agencies may order regulatory fixes if the processing of information is faulty, but must refer the cases to prosecutors if violations of criminal law is suspected.

## 'THIS GOES NO FURTHER...'

### FOLLOWING REVELATIONS ABOUT BUGGING AT THE UNITED NATIONS, IS THERE ANY WAY OF ENSURING THAT YOUR PRIVATE CONVERSATIONS STAY THAT WAY?

News that Kofi Annan and other senior UN figures may have been routinely bugged by US or British security services has caused a huge political row around the world. But it will also have caused alarm among other people in the public eye who deal with sensitive information - or anyone, indeed, who values their privacy. If the secretary general of the United Nations cannot prevent his private conversations from being listened to by all and sundry, who can? It seems if someone wants to listen to what you are saying badly enough, there is very little you can do to stop it.

"Technological advances, particularly in the fields of power supply and miniaturisation, mean that it is now possible to bug almost anywhere and anything," says Charles Shoebridge, a former counter-terrorism intelligence officer.

"Similar advances have enormously improved anti-bugging capabilities too, and an enormous effort has gone into making communications secure - particularly those of governments and even large commercial organisations.

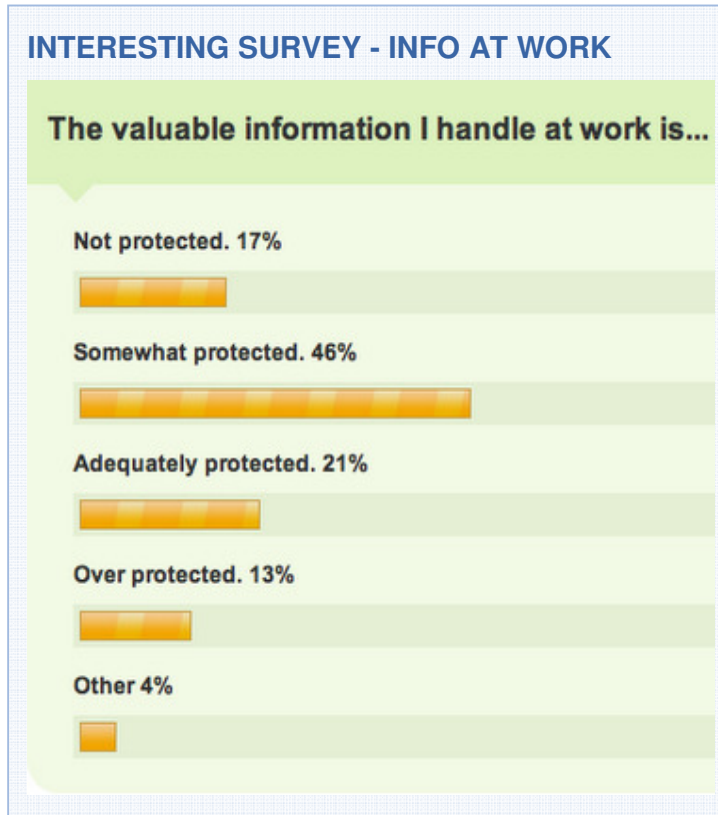


"However, if security is absolutely critical, it will always pay to assume that a conversation is at least capable of being monitored."

### Mobile phones

According to security experts, the most common listening device remains the electronic bug. But government agencies such as the CIA and MI5 have far more advanced systems at their disposal.

Powerful uni-directional microphones can pick up conversations through open windows. If the window is closed, radio waves or a laser beam can be bounced off the glass. The vibrations detected can be translated into speech.



But potentially the most powerful tool for the modern spy is the mobile phone. Mobiles that double as listening devices can be bought over the internet.

### Undetectable

But today's spies are also able to convert conventional phones into bugs without the owners' knowledge. Experts believe this is the most likely method used to gather information in the UN building.

Mobiles communicate with their base station on a frequency separate from the one used for talking. If you have details of the frequencies and encryption codes being used you can listen in to what is being said in the immediate vicinity of any phone in the network.

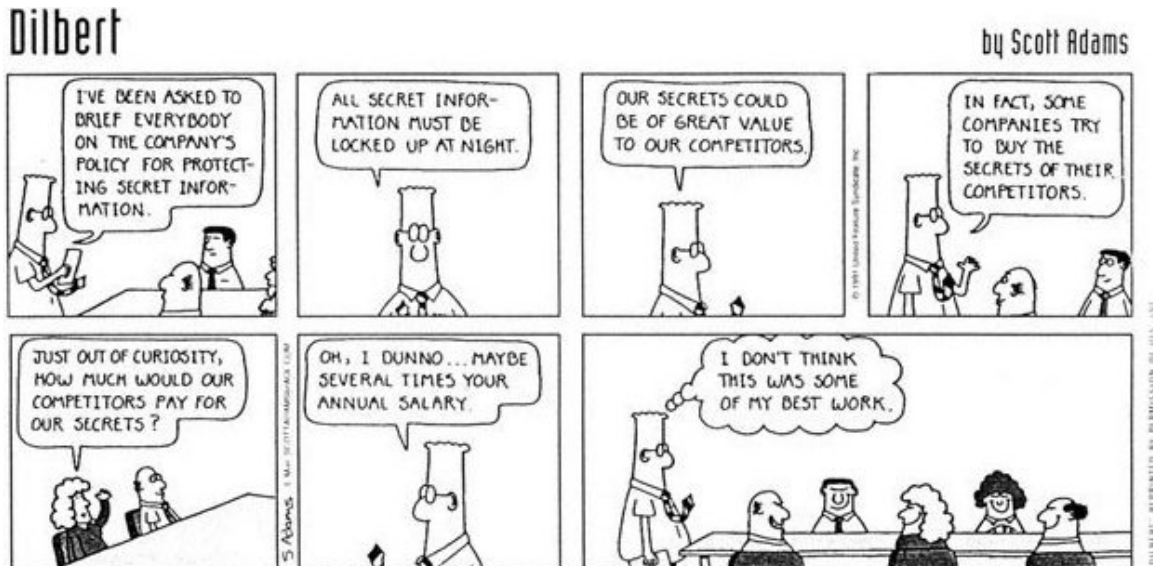
According to some reports, intelligence services do not even need to obtain permission from the networks to get their hands on the codes. So provided it is switched on, a mobile sitting on the desk of a politician or businessman can act as a powerful, undetectable bug. The technology also exists to convert land line telephones into covert listening devices.

## WHAT'S BUGGING THE UNION LEADER? HIS OWN MEMBERS . . .

LEFTWINGERS in a union whose senior members brawled during a barbecue have become embroiled in a new row — by secretly bugging their own general secretary. Hardliners at Aslef, the rail union, allegedly carried out covert recordings of monthly meetings with their Blairite general secretary, Shaun Brady, whom they are trying to oust.

The bugging at Aslef's headquarters in Hampstead, north London, was confirmed yesterday by Keith Norman, who is standing in during Brady's absence. He said: "Because of some of the threats that people say they received from Brady, recordings were made of meetings between him and the executive. He did not know the recordings were being made.

Brady, said: "This is basically entrapment. No meetings are ever recorded in this way and I would not have attended had I known recordings were being made." He alleged that union members also bugged Brendan Barber, the TUC general secretary, during talks about the brawl, a claim that was denied yesterday.



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