Bernie Connor examines the covert surveillance threats faced by officials and business leaders travelling abroad in the age of wearable consumer electronics, and argues that new TSCM technologies and methodologies can now combat this covert information capture

©Getty Images

TSCM IN 2015 – PART 2

WATCH & LEA

A new class of wearable consumer electronic high technology devices has begun to enter the market. The "smart watch" is the leading must-have personal consumer and executive business tool. All of the major players – Samsung, Apple, Sony, LG and Motorola – have released, or intend to release, smart watch products in the near future. Recent history indicates the global take up will be massive. Similarly, while the launch of Google Glass is currently on hold, its potential has energised the consumer world and its ever-demanding search for next generation devices.

The smart watch and similar personal devices acting independently or paired wirelessly with a conventional mobile device are a modern day Trojan horse at any meeting; while security procedures may focus on a "no mobile phone or tablet" policy, these devices could easily enter the fray totally under the radar. A recent UK Government cabinet meeting was interrupted by just such a device, when a reportedly embarrassed Michael Gove had to explain why his newly acquired Christmas present of one of these Smart Watches was regaling all and sundry with his Beyoncé ringtone. It appeared he had diligently handed in all his standard mobile devices – his mobile, his tablet and his PC – as normal, but had seemingly overlooked completely the communication capability of his new smart watch.

In today's world of ever-more integrated and capable communication technologies, we now have a new sophisticated technology that could quite innocently undermine national and corporate information security. For malicious entities, it increases the attack surface massively. The device owner may become an inadvertent "carrier" of an intrusive bug with access to voice, data and video transmissions. A serious new avenue to hacking and covert espionage has therefore been opened up. Accordingly, the potential detrimental economic and strategic consequences of information theft by this means will range from the harmless – where the content is benign – to a priceless and irredeemable loss which could have catastrophic consequences to an individual or organisation.

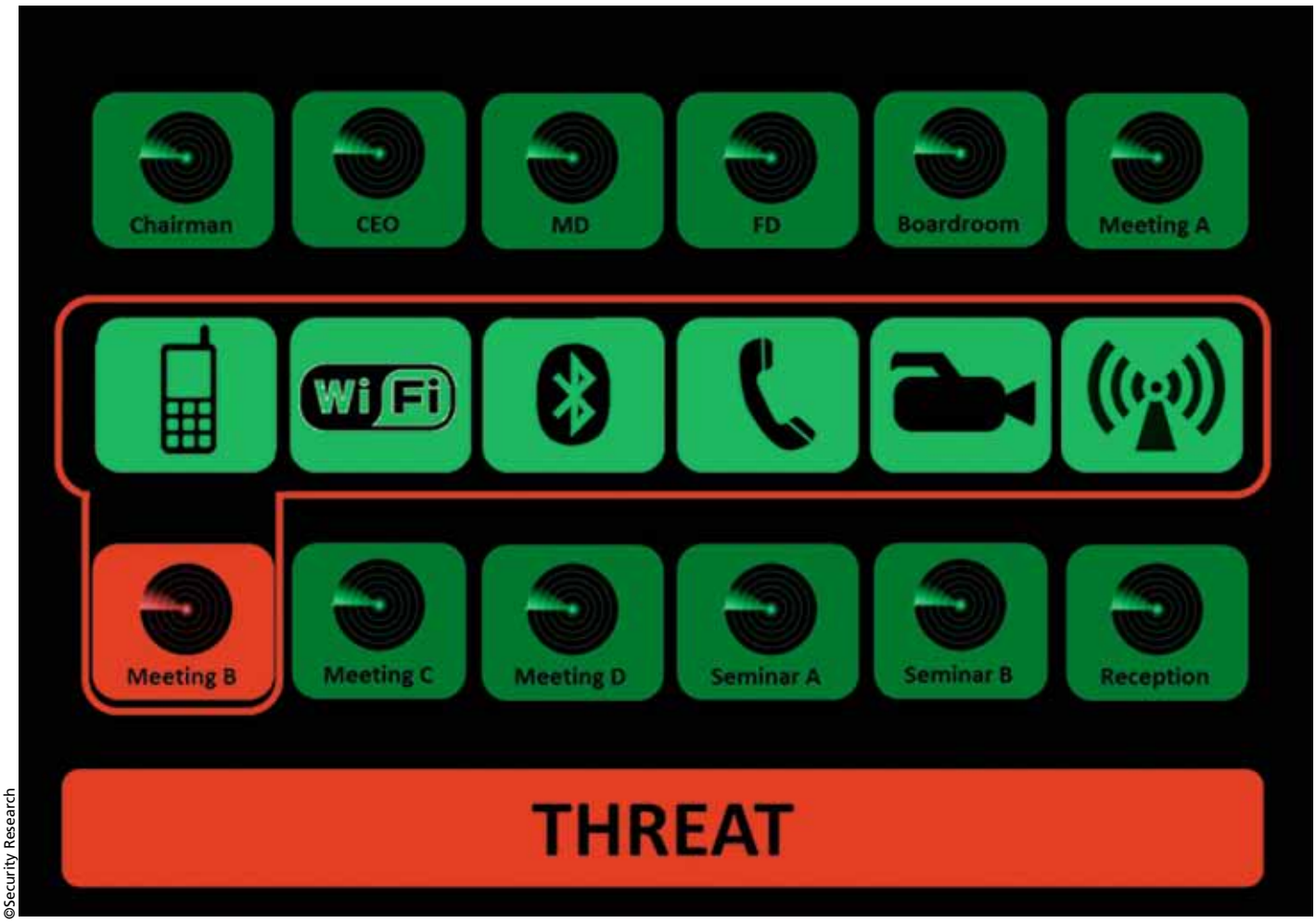
There have been advances in counter-surveillance equipment and systems in recent years, but stubbornly the traditional approach of periodic sweeping of premises remains the bedrock of most security policies. These traditional methods of countering the bugging threat do have limitations, however. For example, they are only as good as the people who do the sweep; they are only as good as the quality of equipment used; they need to be repeated regularly to ensure confidence; and they are always overt and intrusive. It is also important to note that the physical search during a sweep is as important (if not more so) than the electronic search using counter surveillance equipment.

The only sure way to raise the bar with respect to an organisation's response to the eavesdropping threat is to deploy a 24/7 monitoring solution. Such systems provide real-time scanning of all radio channels considered a risk, including analogue, digital, Bluetooth, WiFi and GSM. This monitoring process does require a level of expertise that can be developed in-house through appropriate training, but is often supplied through external monitoring services employing counter surveillance professionals.

In the past 12 months, simple and straightforward user interfaces have become available for these systems that offer a simple traffic light approach to the risk, with the data from the scanning devices processed by a local computer to indicate risk levels as green, amber or red. The levels can easily be monitored by local security team with experts consulted only as and when necessary. These newer systems, deployed in conjunction with periodicprofessional sweeps, provide increased security assurance and decreased risk. The equipment costs can be very quickly recovered by extending the time interval between planned physical sweeps.

But what about when working away from home base when sweep services may not be readily available or are impractical? Multi-million pound tenders are finalised in hotel or rented meeting rooms in parts of the world

"The smart watch and similar personal devices are a modern day Trojan horse at any meeting, which could easily enter the fray under the radar"



©Security Research

where bugging has reached epidemic proportions. Due to local sensitivities or customs issues, it may be difficult or unacceptable to request that the traditional overt sweeps are carried out; even when available, there is always a risk that they will not be completed to the appropriate standards. The only answer currently is to travel with the support of a dedicated, well-equipped security team – which is not only cumbersome but also expensive.

Technological advances in the counter surveillance and electronics industry generated from simpler user interfaces linked to scanners now presents a real opportunity to deploy the next generation of intelligent monitoring systems, however. These systems deploy a miniaturised, powerful, battery-operated scanner that is no larger than a modern mobile phone. This is linked wirelessly to an app running on a standard mobile device such as a iPhone, Android phone or tablet. The technical expertise is provided by the app, which analyses the data in real-time and issues alerts out to any user logged in.

Such systems system also offer protection against the ever-expanding threat from GSM bugs, with the latest now able to differentiate between local mobile phone and data transmissions within "earshot" and transmissions from devices outside "earshot", thereby providing the user with the confidence that all risks are covered and removing the frustration of false alarms. These miniaturised scanners are capable of operating totally unobtrusively, and their portability and size means they can become an essential accessory when travelling away from home. The app-based systems, with their intrinsic modern software algorithms, provide fast, high-confidence warning of bugging when on the road. Without either some form of reliable local sweeping facilities, a counter-surveillance team on hand or the latest innovative 24/7 monitoring systems, you are wide open to the eavesdropping threat.

The risk of espionage and information theft by the covert capture of electronic transmissions is real for all organisations. Bugging in all its forms will continue to be a high-risk threat, and devices that capture data covertly will become more readily available, more effective, of higher quality and therefore more difficult to detect. Recent prolific advances in small and discreet smart watches and other wearable devices, and their vulnerability to hacking, increases this risk significantly.

Regular counter-surveillance sweeps provide some level of security, but the elongated time gaps in between these sweeps serve to increase risk and insecurity. The new generation compact devices operating 24/7 either at or away from home base go a long way to rebuff the renewing cumulative threats and to safeguard confidentiality. Advances in technology are now enabling portable, lightweight, simple-to-use smart products that ensure personal protection from modern bugging threats.

All security teams need to be alert to the danger, open minded to the risks, use the latest technology that is available to them and – it goes without saying – be vigilant at all times. You could say (somewhat tongue in cheek) that "time is not on our side" – so we must be one step ahead of the eavesdroppers and the hackers, and always alert to the enemy within.

The next generation of electronic monitoring systems can provide fast, high-confidence warning of bugging when on the road

Bernie Connor is the CEO of Security Research. He also headed the team that successful delivered a £50m tender for the supply of C-IED handheld detectors to the British Army in 2012/13.