Tony Kingham examines the how cheap, widely available covert surveillance technology is making corporate espionage by employees an increasingly urgent threat

BUGS, ESPIONAGE THREAT

Many agencies now regard the 'insider threat' as the most dangerous threat to the security of government organisations and corporations, and it's not hard to see why. The proliferation of cheap, sophisticated GSM sim-card listening devices available on the Internet makes anyone with a political agenda, a grievance or a commercial motive a potential spy. They could be full time or part time staff or any number of contracted staff like cleaners, maintenance workers, builders or IT support who work in our buildings for years, months, weeks, days, hours or even just a few minutes.

The UK Centre for the Protection of National Infrastructure argues: "The threat from espionage (spying) did not end with the collapse of Soviet communism in the early 1990s. The UK has been and remains a high-priority target for a number of countries looking to obtain information and technologies to help advance their own military, technological, political and economic interests."

GSM devices mean that insiders now have the means available to them to listen-in on conversations in any part of any building they have access to, even if only for a few minutes. Via GSM they can then listen to private conversations from anywhere in the world.

A quick visit to eBay or one of the other online traders will illustrate the point: the cheapest GSM voice activated transmitter this writer found was just $5.09. And there really is something available to fit every would-be spy's pocket and modus operandi, including listening devices and hidden cameras in everything from key fobs, electrical strips, USBs, smoke alarms, digital clocks, phone sockets to computer mice. This writer's personal favourite is the Micro Spy Quardband GSM Listening Two-Way Audio Bug Surveillance Device (GSM Sim Card) N9, firstly because it has a catchy name and secondly because the sales pitch claims: "This two way GSM audio spy device calls you from anywhere in the world when it detects sounds around its vicinity. How awesome is that? Simply insert a GSM SIM card and program it to your desired phone number for call back and start doing your spy business from anywhere in the world." It goes on to say, "You can even place several N9 spy audio devices and set them up at your desired locations like your bedroom, living room, conference room or office. All for only $16.19 with free delivery."

This company is clearly not shy about its target market and what its products are intended for!

There have been high profile cases like Edward

©IPS

©IPS

Corporate espionage can be detected through the use of covert door seals (above right), or uncovered by TSCM professionals during a routine sweep (left)

AND THE INSIDER

Snowdon, the former National Security Agency contractor turned whistleblower, who became the insider threat global sensation by leaking thousands of NSA secrets to media organisations. But the reality of day-to-day espionage is an employee downloading data onto a flash drive or, by way of illustration, the case of a former employee of the Ford car manufacturer who has been accused of surreptitiously planting eight MP3 recorders in rooms around Ford's Dearborn headquarters office in Detroit. Some acts of industrial espionage are carried out for financial gain, some are political and some stem from some sort of grievance.

The Ford case is unusual, not because of the circumstances or the alleged motivation behind it, but because it has come to light at all after Ford called in the FBI to investigate. The reality is that only a tiny proportion of commercial espionage cases are ever uncovered, and if they are, an even smaller proportion are ever reported.

The reason for this is not hard to see. Commercial organisations have shareholders and share value to consider. Breaches in security would inevitably give rise to awkward questions about competence and oversight being asked of the management by shareholders. If serious breaches came to light, they could have a direct effect on share value, potentially wiping millions off the value of big companies. Consequently, most incidents, if discovered, are treated as disciplinary cases and handled internally. The culprit is no doubt threatened with the law, but is instead quietly dismissed.

It is therefore impossible to say how frequently and how seriously organisations are being targeted for this type of espionage, but the sheer scale of the global industry in manufacturing and distributing surveillance devices would indicate that these things are being sold in great numbers and to more than just domestic snoopers and jealous spouses spying on one another.

What we do know for sure is that almost every organisation has been targeted by hackers attempting to steal information through cyber crime activities, which proves that there are plenty of people and organisations out there with criminal intent.

So who is the insider? The insider can be from any function and from any level in the organisation. Some target and join a company with the specific intent of doing harm or committing fraud, but most studies indicate that the insider is usually an existing employee who is either disaffected in some way and seeking some sort of revenge, perhaps for being passed over for promotion or for some other grievance. Or they might simply be an employee who sees an opportunity to commit some sort of fraud and decide to take it. Maybe they have financial troubles or maybe just old fashioned greed. It is therefore almost impossible to profile potential insiders by skill set, job title or seniority.

A report from The Security Company states that the UK's Fraud Prevention Service (CIFAS) estimated the cost of reported fraud to the UK economy alone as £38.4 billion in 2010, and goes on to say that 85 per cent of reported fraud is committed by people within the organisation.

While most organisations are already struggling to put in place some defences against the external hacker, few are doing anything at all to tackle the more dangerous and damaging threat posed by the insider – whether that is through stealing data on a flash drive, or stealing corporate secrets by bugging the board room and meeting rooms.

So what are the latest developments in listening

BUGS, ESPIONAGE AND THE INSIDER THREAT

©IPS

Detection investment: few companies can afford the latest detection systems, so professional sweep teams may guarantee the best level of security

devices? According to Gerry Hall, Managing Director of International Procurement Services, which boasts 25 years' experience supplying countermeasure equipment to government and corporate offices all over the world, the technology is advancing extremely rapidly. "The number and sophistication of devices available on the market has risen exponentially in recent years," he said. "Imagine a Ferrari engineer sitting in on McLaren's race-planning meeting, or an employee from Pepsi sitting in Coca Cola's strategy meeting, or an executive from Samsung sitting in on Apple's pre-launch meeting. Now imagine your nearest competitor sitting in on your board meeting. He doesn't have to be there in person – just a tiny hidden transmitter will do the job.

"Almost daily there are new devices and new ways of hiding them. There's the iPad desktop charger with a hidden GSM audio transmitter, a coat hook with a built-in video camera with a two-millimetre aperture, and from Eastern Europe a piece of cardboard with a device hidden in the cardboard.

"Probably the most worrying are devices like the WiFi Store and Forward transmitters," he continued. "These can be voice, timer or remotely activated and downloaded remotely as well. Download is user-activated, so it means it is terribly difficult to detect. A very long battery life means it can be left in situ for very long periods – anything up to six months.

"Another is the Edic-Mini Tiny 16, a Russian-made recorder that has up to 300 hours of recording time and is only 56x30mm. It even made the Guinness World Records as the world's smallest voice recorder. New models have 4Gb capacity, giving them up to 600 hours recording time. The combination of their tiny size and storage capacity makes these devices a real threat. All this for only $300 on Amazon.

"It takes a professional team with state-of-the-art equipment to find these sorts of devices. Many security companies claim to have TSCM Sweep Teams, but in reality, unless they have at least £50,000 to £100,000 worth of TSCM equipment plus continuous training, they can't do the job.

"There are, of course, those in the corporate world who no doubt think this sort of corporate espionage is either a bit far-fetched or couldn't possibly happen to them, but in a very recent case one of our customers – let us just say a major multi-national corporation – found a device hidden in a radio controlled model truck innocuously sitting on the shelf in their boardroom.

"Fortunately, they take their security very seriously and have invested in the right equipment and training, so the devise was found. Unfortunately, there are many more companies out there that are not so diligent in protecting themselves, their intellectual property and their shareholders."

Tony Kingham has been a journalist, publisher and PR consultant specialising in the defence and security markets for more than 25 years. He is the Communication Director of BORDERPOL, publisher of worldsecurity-index.com and organiser of World BORDERPOL Congress, Critical Infrastructure Protection and Resilience, Europe, Personnel Protection & Safety Europe and Critical Infrastructure and Resilience, Asia.