Espionage – A Modern Day Bug

Editorial Posted 9th January 2015 – By Simon Giddins

If you thought Q's list of inconspicuous devices and covert gadgets were isolated for 007 and the forthcoming James Bond blockbuster, think again. Espionage is alive, well and thriving within private residences and across the commercial / corporate landscape.

Our latest editorial piece has been designed to provide you with a brief insight into this growing trend and to highlight the potential and realistic threats.

History of espionage and bugging

Trading information is as old as organised society and I could dedicate this entire piece to the history of commercial espionage. One of the earliest known incidents is of Father Francois Xavier d'Entrecolles who revealed the manufacturing methods of Chinese porcelain to the Europeans in 1712 and British 18th century industrial developments suspiciously appearing in France whilst the placing of apprenticeships were possibly the first recorded 'insiders'.

The very beginnings of bugging dates back to the American Civil War when telegraph operators sent messages in Morse code, interceptors could literally tap anywhere along the wire and obtain the contents of the message. As telegraphy became more sophisticated, so did the technology to enable eavesdroppers to listen-in, effectively the two have grown-up and evolved side by side. Fast forward to the Cold War, which could also be described as a very hot war in the use of espionage, one infamous case in 1952, which saw the Soviet

present U.S. representatives a carved wooden replica of the Great Seal of the United States. It hung prominently within the US ambassadors study for many years, before a tiny microphone was found in the eagle. The small device was capable of being activated by an electronic ray from outside the building and for its day represented a fantastically advanced piece of applied electronics.

Such monitoring techniques have been regularly discovered. In 1984, an unsecured shipment of typewriters for the Moscow Embassy had been bugged and had been transmitting intelligence data for years and just one year later, newspapers revealed that the Russian Intelligence Services were using invisible 'spydust' to facilitate tracking and monitoring of US diplomats.

In recent years we have seen the Norwegian police investigate a possible spying operation by a 'foreign power' following the discovery of electronic devices, which were designed to intercept telephone conversations near government buildings. The FBI launching an investigation into a recently fired Ford employee for allegedly placing listening devices in the Ford offices. In 2008 the House of Commons office of Damian Green, the then Tory' immigration spokesman, was routinely swept for electronic bugging devices, along with other offices belonging to senior Conservatives, amid fears of covert monitoring. It is not known whether a covert device was ever found during these searches. But if the suspicions were ever proved right, it would have held major implications for the protection of parliamentary privilege. And in 2010, one of the world's highest-paid businesswomen allegedly hired private investigators to plant secret surveillance devices at her estranged husband's £2 million home.

These are just to name a very small few.

Current trends and threats

Should business owners, high profile individuals or the affluent be paranoid and protect everything from product information to their movements or anything, in fact, which could award their competitors the edge or ammunition for a suspicious partner?

Espionage is a growing trend and fuelled by sophisticated technology. The cost of fraud to the UK economy was estimated by the UK's Fraud Prevention Service (CIFAS) to be a massive £38.4 billion in 2010 and perhaps an even further sobering thought is that 85% of those committing such transgressions did so from within the organisation. The insider threat is very real.

And it's not confined to the commercial sphere, technical surveillance is undergoing a boom and is infiltrating people's private lives with some of the most trusted individuals or staff members potentially the perpetrator.

In December 2014 a man in Surrey was convicted of reconfiguring CCTV cameras to spy on his estranged wife and children. Whilst disturbingly, a doctor was jailed for using technical surveillance equipment in toilet cubicles to watch friends, colleagues and patients using a sophisticated network of covert cameras. Meanwhile, the former Managing Director of Leeds United Football Club instructed the installation of covert cameras in to the club boardroom and toilets following reports which he received alleging the misuse of Class A drugs within the club.

What's available?

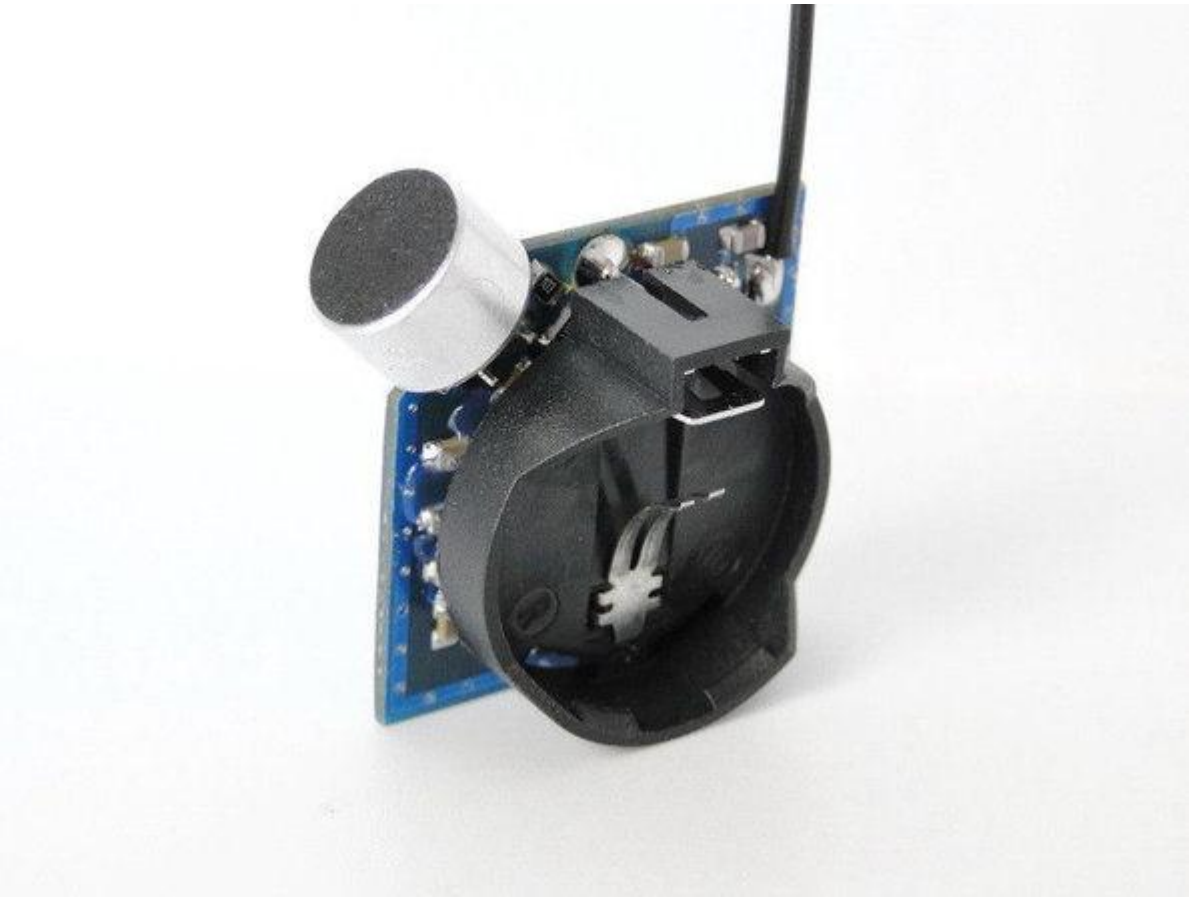
Devices you (or your competitors or partner) can pick up at minimal cost are many whilst estimates place the value of eavesdropping device sales at an incredible £10 million in the UK, providing an indication of the extent of surveillance equipment which includes GSM bugging devices enabling the user to silently listen to calls.

Gadgets are readily available to enable even the most amateur 'spy' to commit commercial espionage or stalk their partners, whilst drones and quadcopters,(remote controlled flying devices with cameras which run off smartphone GPS) may have been developed for the hobbyist market, are now being used for more sinister practices, with would be burglars taking to the safety of the skies to obtain a holistic view of property, clearly identifying items of interest or areas of vulnerability

A quick search for GSM devices on eBay or even Amazon today indicates that, large amounts of these covert devices are being sold monthly. One seller who is currently selling a 5 pack of 'Covert Mini Bug Listening Surveillance Devices for £24.99 has sold over 480 of these packs. A five minute browse through this section reveals that hundreds are sold each month. Raising the questions; by who and for what reason?

Martin Quaife, Blackstone Consultancy's technical surveillance advisor comments:
"Listening devices on the open market range from simple products such as baby monitors to those which are very small and discreet, but highly effective, even over long ranges. Placing the transmitter in one room is easy and it is likely nobody would know. Dictaphones

are used widely and can be slipped into the inside pocket of a jacket before entering a meeting. The clarity of the voice recording is amazing, trust me I know!



"Meanwhile, GSM mobile technology can be used in many ways, for example, a unit can be built into an extension lead or a socket, even a mobile phone charger or e-cigarette and all the individual needs to do is insert an active sim-card, dial in and listen. It is even possible to buy a mobile phone that has been altered, to the human eye it's a normal handset and would never raise suspicions, but it allows someone else to listen-in undetected. Other transmitting equipment can be activated remotely and with long battery lives can be in place for as long as six months.

One of Blackstone Consultancy's approved TSCM service providers for the Middle East and Africa, Stuart Thompson, managing director of Advanced Security Protection based in Dubai, said: "The past 15 years has seen a radical advancement in technologies such as GSM, Wi-Fi, Bluetooth, GPS and micro-video; thus giving rise to a wide variety of new smaller, more reliable, off-the-shelf surveillance products. This is further exacerbated by unregulated online sellers such as Alibaba and specialist online 'spy shops', where illegal eavesdropping devices can be purchased for as little as £30.00 (US$ 45.00). The scary part is that everybody now has easy access to these devices and that given their relative simplicity to operate, anybody can use them from any corner of the globe."

An article in The Telegraph explored more unconventional hiding places for devices including a high-speed camera and a packet of crisps whose vibrations were translated into

audible sounds and even bugs of the insect variety whose brains were 'bugged' and remotely controlled

Who's bugging you?

The answer is short and far-reaching. It could, quite literally be anyone. Anyone who has a vested interest in obtaining intimate information about you as well as your personal and business life. It could be your spouse, any member of your family, so-called friends, your house-staff or the affable guy you employed last week. Technical Surveillance has evolved from the standard company/individual bugging one another, to information brokers. Individuals who will steal technical or personal information and then sell it to the highest bidder, where there has been an acrimonious divorce or a custody battle is fertile ground. We received several enquiries last year from four European cities, where former spouses living in properties that formed part of the divorce settlement believed their former partners were watching them, inevitably and sadly in each case, they were. Devices were already fitted in the property or staff members had been coerced into placing them.

What you can do about it?

An extensive threat thereby needs a far-reaching, often complex and multi-layered solution. Ranging from educating employees and staff to implementing counter surveillance including technical surveillance countermeasures (TSCM or bug sweeping – any eBay purchases will soon be identified by an expert team utilising the latest equipment), actions could also include physical security underpinned by specialist training. It is advisable to implement measures before a commercial espionage attack occurs, meeting the threat head on. If necessary, take robust action against perpetrators and don't be afraid to call in the police, it instils confidence and by so doing, naturally increases the awareness of employees who will therefore be more likely to deter further attacks and less likely to be tempted into espionage.

New state-of-the-art GSM and Wi-Fi 'store [record] and forward' devices have added a new dynamic to the sweep, as these devices only transmit for around five minutes per day in order to send up to 24 hours of recorded audio data. Likewise, there appears to be a growing trend in the use of relatively inexpensive GPS tracking devices, which can be placed in, or underneath a vehicle and are now so small, they can also be easily hidden in a person's handbag, rucksack or luggage. Listening, videoing and tracking device technologies have evolved at a rapid rate, especially in the areas of size, recording quality, RF shielding and extended battery life. However, a professional TSCM service provider will have purchased advanced up-to-date TSCM equipment and honed their skills accordingly to meet the challenges of the current day electronic eavesdropper.

Appointing a reputable and highly trained team to undertake a TSCM survey is a start whether it's for your home or workplace. A reputable company will not only have the correct equipment but understands how each piece of kit complements another Our sweep teams encourage the client to ask questions and happily explain what each item of equipment is for and its purpose. If possible, ask for a recommendation or at the very least, ask the company for references and follow them up.

Visit the ASP Website: http://www.advancedsecurityprotection.com/services/technical-surveillance-countermeasures-tscm-debugging