Residential TSCM

Confidentiality Assurance for Executives, Directors & High-Profile Individuals

The home is increasingly becoming the primary working location for many individuals, while a far greater proportion of the workforce are now spending more of their working week in their home environment.

For the C-suite and senior executives, home working has always had a higher take-up (over double compared to the rate for administrative workers according to research undertaken by the TUC in 2019), and with the recent Coronavirus pandemic, this trend is only predicted to escalate.

The Challenge for Security Assurance

Whether you are responsible for physical and information security, or a Director or individual who has become aware of a threat to your information confidentiality, it is clear that there is now the need to assess and ensure the integrity of the home office in the same way as that of the work office environment.

Often front of mind due to their frequency and reporting in the media is the threat of cyber-attacks. Consequently, an assessment of IT hardware and software protection and the availability of education and training into current threats are routinely undertaken. However, how effective are these assessments and controls in isolation when the determined adversary is still employing the traditional espionage techniques?

In much the same way as cybercriminals are becoming more sophisticated, the eavesdropper is also learning and adapting to the changes in working practices. With the strategic level of conversation taking place by the C-suite and the highly sensitive nature of some roles or the industries they operate within, the home environment is now a prime target for an attack and adversaries are seeking to infiltrate home offices in the same way as an office building environment.

The Threats Posed to Private Residences

Private homes and residences by their nature have lower levels of access granted to them by the public. However, the following threats remain:

- Planting of a listening device by a third party into the home, private vehicle or computer hardware. However far-fetched this may sound, the threat is very real. Retained staff or visitors with access to executive homes are susceptible to bribery and means of intimidation to plant devices on behalf of those wishing to listen in to sensitive conversations.
- The unintentional introduction of a disguised device from outside the home, e.g. within a corporate gift.
- Radio Frequency interception to listen in and steal information sent via unsecured WiFi, telephones and mobile phones. In addition, an unsecure WIFI can allow eavesdroppers to gather information the connected devices.
- Devices attached to computers to enable remote control.
- A GPS tracker attached to your vehicle or an electronic eavesdropping device planted in your vehicle, allowing an eavesdropper to gather information about your movements, contacts and private conversations.

In order to provide assurance that security has not been compromised and to assess the risk of an eavesdropping attack in the future, a security review of the residence including technical surveillance countermeasures (TSCM) survey is highly recommended. By taking a proactive approach, the risk of data loss or compromise is minimised and the potentially devastating impact of highly sensitive information falling into the hands of a competitor or undesirable third party is avoided.

How Esoteric Ltd Can Help

From large estates, to executive homes, Esoteric's residential TSCM services are a wise choice to help protect your privacy, personal information and your security. As world-leading counter-espionage and countersurveillance experts, we offer a range of services to help assure the confidentiality of private residences..

Technical Surveillance Countermeasures (TSCM) Surveys

Using the latest in counter-surveillance technology, Esoteric Ltd conduct TSCM surveys to detect and prevent theft of sensitive information by illicit electronic surveillance, electronic bugs and eavesdropping devices.

Electromagnetic Egress Review

Homes are susceptible to signal leakage or electromagnetic egress from sources such as WiFi, telephones, mobile phones or computer hardware. These can be intercepted by adversaries to steal critical information. Esoteric Ltd can identify and assess these vulnerabilities and ultimately recommend how to protect the home office against them.

Physical & IT Security Review

To understand the vulnerabilities of a home office to eavesdropping attacks and to put measures in place to deter and protect against them, Esoteric can provide full information security reviews, either of the physical or IT security or both. Once the physical or IT environment have been assessed, practical recommendations are offered to address identified vulnerabilities and risks to information confidentiality.

Get In Touch

Esoteric Ltd has over 20 years of experience in offering a confidential and discreet service to a highly professional standard, and is trusted by organisations, governments and individuals across the world to assure information confidentiality. Accredited to National Security Inspectorate Gold standard and holding ISO 27001 status, Esoteric personnel are all cleared to minimum BS7858:2012 and we employ specialist engineers from military and police backgrounds to use the latest TSCM equipment and techniques.

esoteric

www.esotericltd.com

UK
Links 2, The Links Business Centre
Old Woking Road, Old Woking
Surrey GU22 8BF
+44 (0)1483 740423
mail@esotericltd.com

UAE
PO Box 338594
Dubai
+971 56 3899 432
mail@esoteric.ae