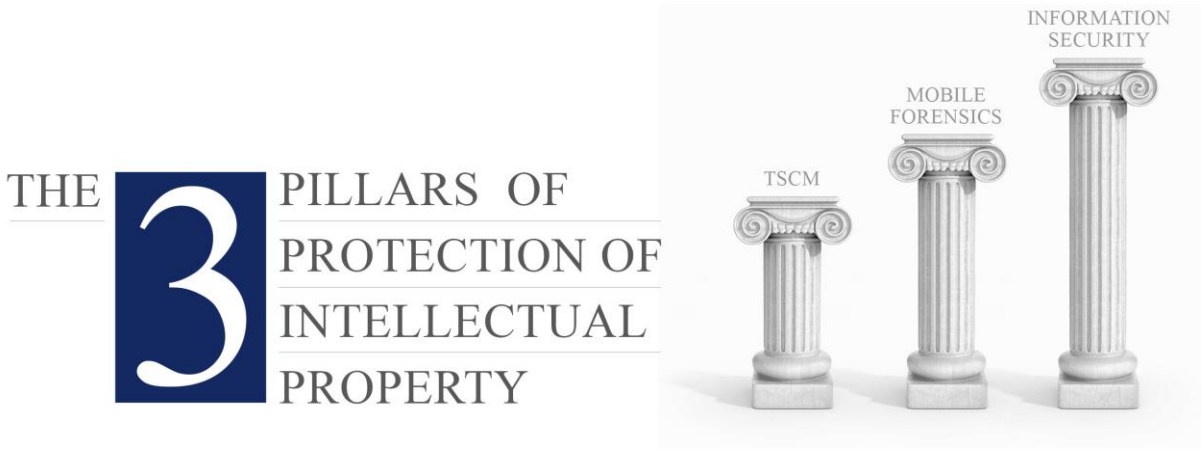


TSCM | MOBILE FORENSICS | INFORMATION SECURITY

Protocols and Procedures to Safeguard your Intellectual Property.

On almost any given day it is easy to find a story in the press reporting various types of listening devices, cybercrime, cyber espionage or even cyber warfare. It is easy to see why cybercrime and espionage are so attractive to criminals and governments alike.

So, unless you have lived in a cave for the past five years, most people are aware of cyber threats and this is especially true among government and corporate circles.

What is not so widely understood, is that old-fashioned human spying by people from the inside and outside an organisation, is still a very real threat and why that threat is to continue.

A well- informed and well-placed insider may be able to access information that has not been hackable because, for example, it is "air gap" protected.

Technological advances have made spying cheap and easy, which means almost anyone can become a spy if they have the right political or financial motivation.

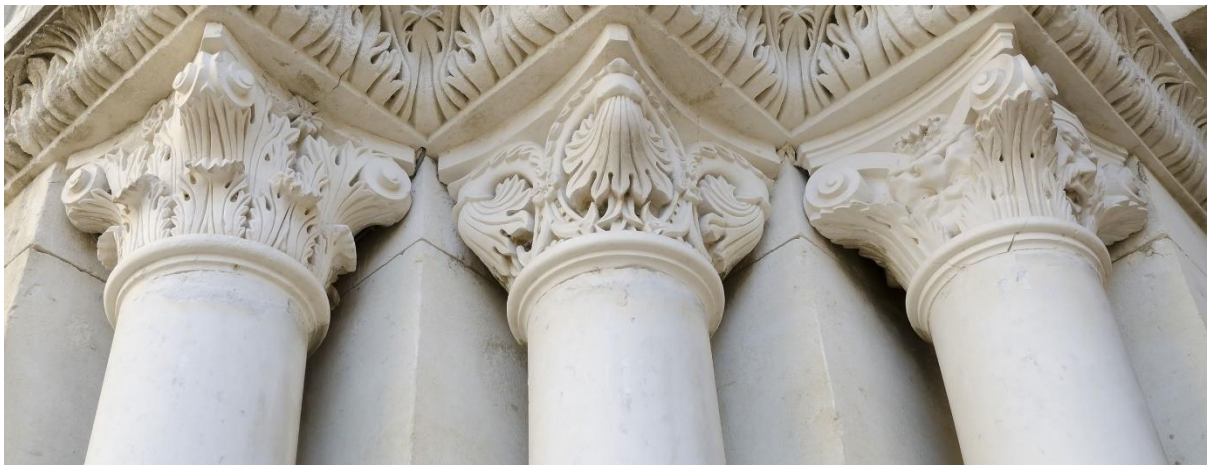
Human spies are also able to provide information that is not necessarily held in any database. Like gossip about the member of the team may have financial or marital problems that leave them vulnerable to blackmail and coercion. Private conversations in the board room, on the phone or in the office kitchen. Conversations, opinions and ideas which may impact on the outcome of a given set of circumstances whether that's on political, financial or national security issue.

Some have motion sensors that activate when someone enters a room, ideal for the boardroom or meeting rooms.

This is especially true of GSM Technology. Surveillance tools can now be hidden in enormous variety of household goods like phones, power strips, light bulbs, alarm clocks, digital music players, power adaptors, smoke detectors and many more. Using your GSM phone, you can call into your surveillance device from anywhere and conduct covert room monitoring without anyone knowing. You can hear and record all conversations within range and when you're finished simply hang up.

All organisations are potentially vulnerable!!!

Avaricious or disgruntled employee, contact workers or maybe even the photo copier repair man or women. Anyone that has access to your building can leave the device and leave you vulnerable to surveillance.



So what can be done?????

Advanced Corporate Solution has been working with government agencies, international companies and high net worth individuals supplying Security Solutions, Debugging Sweep Team services, Countermeasures and Consultancy for more than 23 years.

“No organisation can ever be totally secure, especially when people are coming and going, but it is important to set out your security priorities and establish protocols.

Setting protocols – For instance, defining and documenting what sort of information constitutes sensitive and secret lays out where when and in what context discussions about this information should be had. This includes rules about telephone conversations on both landlines and mobiles.

It could be argued that all internal information within an organisation is proprietary and therefor sensitive and secret, but is just good sense to make special consideration for high value information and make everyone who is legitimately involved aware of the special rules that apply to it. Practical measures that can be taken include establishing secure areas. These can be permanent such as boardroom or CEO’s office or temporary such as hotel rooms. These areas must be swept for devices on a regular basis to ensure that they are clear and free of surveillance.

Now you can do this internally by specially trained members of your own staff, but they must be properly trained and have the right equipment which is expensive. As a guideline the minimum would be a Non-linear Junction Detector, TSCM Spectrum Analyzer such as the Osco Blue, Raptor, Andre Deluxe, Talan etc.

The answer: Contact Advanced Corporate Solutions which provides a specialist sweep team with the correct equipment, training and years of experience.

PLEASE BE AWARE, IF YOUR SWEEP TEAM DOES NOT HAVE THE RIGHT EQUIPMENT YOU WILL BE WASTING MONEY AND COULD BE COMPROMISING YOUR SECURITY.