

## SHEARWATER TSCM

Science and Innovation Centre  
Station X, Bletchley Park  
Sherwood Drive  
Milton Keynes  
MK3 6DS UK

Tel +44(0)1908 677062  
Fax +44(0)1908 230732  
Mob +44(0)7836 521376  
Email [info@shearwatertscm.com](mailto:info@shearwatertscm.com)  
Web [www.shearwatertscm.com](http://www.shearwatertscm.com)



### If you think you might be vulnerable, what should you do?

Well first of all think about it, and then think again. We know that there are some very real threats; we're dealing with them every day. You would be surprised which individuals and companies are being attacked, but that is of course confidential. This might help your thinking. For a technical clandestine attack to exist three factors need to be present:

#### ASSET RISK THREAT

Are any of your Information Assets of **High Value**? Are these Assets at **Risk** – would anyone else like to share them? Is there a **Threat** – is there anyone out there with the inclination to steal your Information Assets?

If the answer to any of these three questions is 'Yes', read on. Otherwise save your time and stop now.

You're reading on, so you have a potential problem, so start your thinking by getting these four words in your mind:

#### What? Where? When? How?

**What?** is questions that you have just answered.

**Where** might you be attacked? It could be the Boardroom, or an office, or your laptop, or at home (regarded as a Soft Target and very vulnerable).

**When** may you be attacked? Well it's pretty obvious that it is most likely to be when you are dealing with critical information. Is it at your office or do you also deal with work elsewhere, in your car, or at home? If the attack is tied to a location, it will probably be the Boardroom or some critical office, but as employees regrettably aid the majority of attacks, it may well be that the 'bug' is removed at night to change the batteries.

This means that some of the **Defence Strategy** needs to be **Covert** and **Real-Time**.

**How** could you be attacked? It could be a basic Audio Link, a wired microphone possibly using some of the redundant cabling in your building. This is the first choice of the professional assault teams because despite being Low Technology it yields high quality information and is reliable. Or it could be the highly sophisticated, High Technology microwave communication systems that until recently were battlefield classified, but are now available over the counter. Or it could be anything in between or outside these parameters. If you can decide What? Where? When? and How? you have to develop a **Strategy**. There are no simple one-click answers

here, the **Defence** must be in **Depth**. You'll not be surprised to know that we call it a '**Defence in Depth**' strategy.

This means that you should really consider having at least two independent defences against any assessed risk so that there is a comprehensive inherent back up. It also means that you have to be sure that you remain abreast with a technology that is developing at an amazing pace. So what can be done?

Well if you've worked out the What? Where? When? and How? you will also need to **develop** a '**Defence in Breadth**' strategy.

- 1 Do you constantly monitor all possible attacks at all conceivable locations?
- 2 Do you go for periodic sweeps of all probable locations?
- 3 Do you sweep some and monitor others?
- 4 Do you think that this is all too much and hope that there's really no need to do anything at all?

It's really a simple question of **Risk Assessment**.

Well if your answer is (1), you'll do nothing but monitor, to the exclusion of all other business activities. If it's (2) you're making progress if your risk assessment is totally accurate and you are sure that you have at least two different ways to detect every conceivable current threat. If it's (3) you're beginning to develop a realistic and useful strategy, but you may need advice and support. If it's (4) you're wasting your time reading this.

#### So how can it be done?

Our experience at **Shearwater** is that security measures are only successful if they are driven from the top. If Top Management regard the issues seriously and include them as regular agenda items, then things happen. You need a '**Top Down**' approach. **Shearwater TSCM** has vast experience and capability. We can help you to assess your risks and develop top down strategies in breadth and depth. A **three dimensional approach**; Top Down, Breadth and Depth.

We have no interest in amateur superficial quick fixes – they don't work. Our very successful business is founded on long-term relationships, arising from high-quality solutions based upon unparalleled experience. Successful defence is cost effective, there's no such thing as a nearly successful defence, that is actual failure.

***We aim to be the best, and our ongoing development program keeps us as good as it gets.***

## SUMMARY

### **Defence Strategy**

- Three Dimensional approach:
- Top Down Philosophy
- Defence in Breadth

Defence in Depth Defence in Breadth: Low to High technology, Audio to Microwave to Video **Defence Equipment**

- Real-Time monitoring capability.
- Covert operation

Overlapping capability to ensure seamless defence and intrinsic back up.

If you still have questions please contact us at Shearwater TSCM.