



## **SECURITY CONSORTIUM INTERNATIONAL LIMITED**

**HEAD OFFICE: 33 BURY STREET, ST JAMES'S, LONDON SW1Y 6AX**

### **QUANTITATIVE THREAT ANALYSIS**

#### **TRADITIONAL METHODS OF THREAT ANALYSIS**

Threat analysis has traditionally been extremely difficult to quantify. Many notable threat analysis consultancies still describe threat as either "high or "low" against a list of possible crimes and business threat.

#### **THE IMPORTANCE OF QUANTIFYING THREAT**

The quantified level of any analysis may lead to many thousands of pounds being spent on preventive security equipment or guarding without a clear understanding of the true cost or extent of that threat occurring.

#### **NEW METHODS OF THREAT ANALYSIS**

SCI have applied a number of modern and sophisticated techniques to produce a clear and quantifiable analysis of risk.

These new methods of analysis are on three levels:

##### **Level 1      Vulnerability and Probability Analysis**

At the first stage this process examines every type of risk faced by a business and then quantifies firstly the cost of failure and the probability of occurrence to provide a simple threat matrix which can be automatically prioritised.

The output is in tabular form as a costed and prioritised set of threat conditions and their counter measures.

##### **Level 2      Dependency Modeling DMT & RAT**

This technique starts from the opposite end of the problem. It does not look at any particular threats but starts with an assessment of each functional area of the business in its working mode. The cost and length of time to temporarily or permanently replace any function of the business is evaluated to calculate:

- (a) The cost of replacement of the function.
- (b) The cost of consequential damage while the function is out of commission

These costs are then directly balanced against the costs of any proposed counter measure until an acceptable balance of cost versus consequence is achieved.

The output is in the form of a computerised analysis of the cost of the loss of a function of the business versus the cost of counter measures. The software tool is provided to the client as part of the service and the process can be updated continuously thereafter by the client.

### **Level 3 Protection Requirements Model**

This highly sophisticated computerised analysis technique provides high definition coloured maps of any area such as an airport or petrochemical plant as a visual histogram of risk. The programme can be re-run to show any particular type of threat in map histogram form such as:

- Time to penetrate to any part of the site.
- Distance to any part of the site.
- Probability of detection of an intruder.
- The cost and consequence of any breach of security
- The effect of reduced consequence as each counter measure is added. eg fencing, lighting, CCTV, barrier detectors.
- The exact reduction of risk by the use of any particular security device at a given location.
- The output is in the form of visual maps or mathematical tables of risk, detection, time, distance, cost and consequence as well as any other relevant variables.

The method is flexible enough to cope with any kind of preventive device or people over site areas from 250 kms of coast or border to 60 acre petrochemical sites and airports.

The above three methods provide the total solution for the accurate assessment of risk for projects to suit any budget and level of security. Vague statements of risk are a product of the past. These methods provide clear, accurate, visual means of assessing risk in all areas of business operations.

**Further details about the Consortium can be obtained from  
Chris Gordon-Wilson in the UK:**

**Tel: 0044-207 839 2888**

**Fax: 0044 207 839 6888**

**e-mail: [security.consortium@btinternet.com](mailto:security.consortium@btinternet.com)  
or see our Web Site at: [www.sciltd.co.uk](http://www.sciltd.co.uk)**