

Service provision for an Internal Management Threat Analysis (IMTA) [aka “The Resilience Matrix”]

Resilience Matrix Overview

Our approach, using a Resilience Matrix, is to produce a fingerprint of how well an organisation’s arrangements will deal with threats to its internal processes and activities. These threats can be business related failures such as loss of an asset, inefficient process or supply chain integrity as well as targeting actions such as those arising from terrorism.

The performance or ‘utility’ of the organisation against these threats is shown on a 3x3 matrix (known as an “effects matrix”), where the columns of the matrix represent the utility of the organisation with respect to its People, its Processes and its Physical assets and the rows represent the utility with respect to where these are targeted in terms of Prevention, Preparation and Protection.

By comparing the shape of the completed matrices across similar or related threats, the technique also allows for the assessment of Resilience within an organisation. This is especially true where the opportunity is taken to focus on the working relationship between different levels of employees (white and blue collar) and to examine their interdependencies.

Evaluating the organisation according to the effects matrix defined above, and in particular the ‘People’ column also provides for the identification of Human Factors with an impact upon threat management.

It is the overall shape and balance of the completed matrices which provides the organisation’s ‘fingerprint’ or its Resilience Matrix.

Method of Application

The key to application of the approach is to first identify the range and type of threats that the organisation wishes to assess and the type of impacts which are to be considered. For example, the threats could be internal (e.g. arising from failure of in-house systems or process or from human failures) or they can be external (e.g. failure of a supplier or as a result of targeted activity or terrorism) and the impacts could be loss of business, loss of assets, loss of reputation or loss of life.

The process is dependent on the Resilience Matrix Team having access to all levels of management and departments (perhaps “shop floor”) (assuming both are to be included in the Resilience Matrix). A pre-requisite is that each department or level in the organisation is reviewed independently and the results are evaluated via algorithms in the Resilience Matrix thereby removing human or emotional influence to provide a rational picture for the senior management to consider. The process, where necessary is confidential for each individual taking part in the review.

Once the range and type of threats has been agreed a Taxonomy of Threats is produced to focus the assessment;

Taxonomy of Threats: An example taxonomy could be Strategic (Corporate) or Tactical (Departmental); the key target for the threat; the entity initiating the threat, be they an external party or an industry insider or an external party with assistance from an insider; the motive for the threat be it profit – as for theft or political or ideological as for an act of terrorism; and finally the timeline for the act whether planned, in which case some further activity like computer hacking may have taken place or a spontaneous and/or opportunistic act.

Once the Taxonomy is agreed a representative range of threats is agreed and these are prioritised;

Prioritisation of threats within the organisation: The Resilience Matrix approach is to then look at each threat and to ask, in the absence of any safeguards or arrangements, what is the relative “attractiveness of the threat to the perpetrator (whether intentional or by default)” and the what is the relative “ease of implementation” (whether intentional or by default). The Team is then able to focus on those threats identified as being a priority.

The Team then creates a Threat Tree that shows the sequences of actions / failures needed to achieve a Goal.

The Threat Tree: Threat Trees put the threats into perspective showing how “Needs” to accomplish a threat are logically connected through “AND” Gates and “OR” Gates.

Threat Control Ratings are then assigned to the Effects Matrices

Threat Control Rating: Having built the “Threat Trees” scoring takes place using information from stakeholders and experts. Identifying a step within the chosen process of the department; Identifying “How could it be realised in the absence of any security measures?” Asking what the “Needs” are for the perpetrator; we ask what controls the organisation has in place to stop the perpetrator; we ask where they sit in the Effects Matrix structure. Lastly we ask how effective are the controls and give them a rating. The stakeholders can be drawn from different levels within the organisation and results compared across these. Also, comparisons between similar threats can be used to draw out subtle dependencies.

Finally we construct graphical representations of the results using Security Trees.

Security Tree: Using the information from the Threat Control Rating we create a Security Tree colour coded to demonstrate the deficiencies or effectiveness of the controls in place.

The Security Trees and Resilience Matrices can then be used to increase the resilience of the organisation to minimise or mitigate the threats as an internal exercise.

Dominic Kelly (Managing Director):
Nigel Hale (Technical Director):

dominic.kelly@cbrneltd.com
nigel.hale@cbrneltd.com