

## **Establishing a suppliers resilience**

There has been a great deal of discussion recently in a number of online forums and groups on how to establish the status of a supplier with regard to its capacity to recover from a disaster and its general resilience.

A critical supplier ticking the box of a questionnaire asking if they have policies for health & safety, crisis management, information security, Business Continuity etc is common place but can be of little value unless it is followed up by a request to see such polices and further for them to supply evidence that they are actually implemented across their organisation.

Agreed the request to supply such evidence can often cause misunderstanding and confusion for example a customer may demand to review any plans created to deal with a crisis and so feel assured that the supplier would survive and fully recover from any disaster which may befall them. The supplier on the other hand may feel justified in refusing to disclose such plans as their content will contain information of a secure nature to them and their business.

So does a customer really need to view such plans? I believe not. Indeed a refusal to provide these could well be interpreted that it demonstrates the business have a very positive security position and a clear policy on not divulging information which could place their business at risk. I have worked with several global organisations who will not share their plans with a customer no matter how important to them.

However, what should be expected, and these organisations were willing to provide this, is for them to readily provide a body of evidence which clearly demonstrates such plans exist, are current, regularly reviewed, exercised and any actions emanating from these exercises closed within a clear and reasonable time frame.

Thus the information or 'body of evidence' provided could simply consist of the following information

1. The front cover of any plans or procedures: I would expect such documents to have simple document management included in them.

For example.

- a. The document version
- b. The date it was created
- c. The date it was modified.
- d. The name of the person who approved its use

Any lack of document control indicates an organisation that is in turn not in control of its business. Alternatively there maybe a demonstration of control but this can be verified simply by how periodically the document has been updated or was it created so long ago as to be of little current value.

2. The most useful document to review is the exercise schedule of any plan and from it one can discern the following:
  - a. How often the plan is exercised.
  - b. When it was last exercised.
  - c. How many actions were created as a result of that exercise.
  - d. Whether these actions were closed in a timely manner.

As can be seen one does not need to view the details of the exercise and resultant actions just proof that they took place and resulting follow up work was completed.

3. I also would request the name of the person and their qualifications who created these plans. Having an unqualified or trained person who is simply good at writing documents adds little value to a company's resilience.
4. Finally I would request the opportunity to observe an exercise. Doing this as part of a teleconference is often sufficient as by careful listening one can often establish whether or not the exercise team understand their roles and responsibilities in the event of a crisis.

To close I would stress just how important the personal relationships with a critical supplier can be. Good relationships create trust and understanding between parties at times of stress rather than suspicion and mistrust the alternative can bring.