

## “MANAGING INFO IN THE INFORMATION AGE”

***“Our challenge today is to know what information is relevant when investigating an incident. Data presented are normally so voluminous and blurred that we are confused and overwhelmed.”***(Gordon Tracy – VP Client Platforms, Aviation Software Platform Provider)

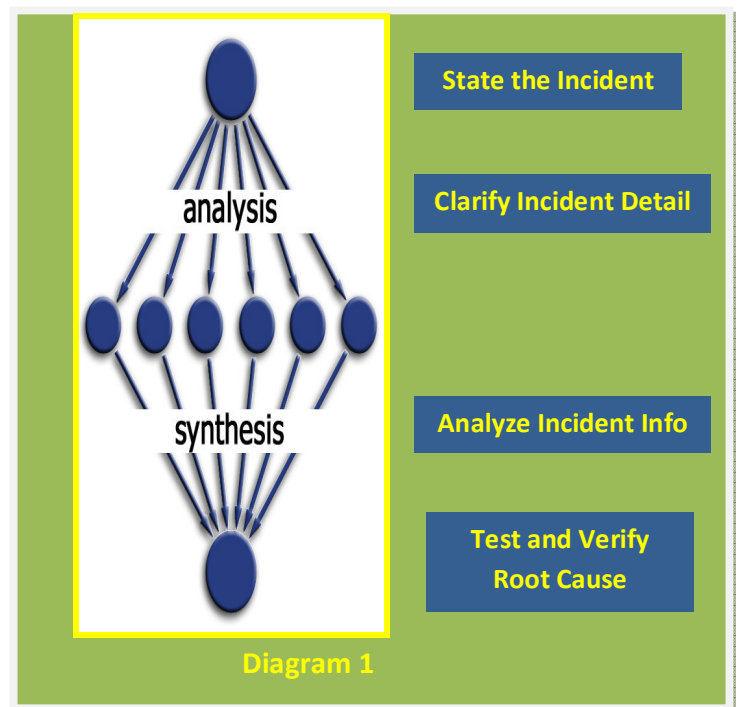
There are six deadly IT habits, which collectively degrade information needed for an effective incident investigation. They are:

1. Trying to solve multiple faults in an incident
2. Not being sufficiently specific when gathering data
3. Not consulting the correct information sources
4. Not “ring fencing” data to create a contrast, elevating data to information
5. Not working with minimalistic information
6. Not having a robust method for testing causal theories

The above habits practiced singularly or in combination, will lead an investigation team to create too many possible causes. This, in turn, will result in many hours of replication, as well as wasted time and money before arriving at the root cause of the problem situation.

Let’s investigate each pitfall and provide you with examples and guidelines on how to avoid each deadly habit:

1. **Trying to solve multiple faults in an incident** – An incident generally presents itself in a “multiple faults” fashion such as: “Servers have performance issues and freeze now and then” – Unless you are 100% sure that the two faults mentioned are caused by the same cause, you should not deal with them simultaneously. In our experience, this is a major cause of



“analysis paralysis”, circular discussions and confusion. You need to investigate one fault at a time to ensure a focused analysis.

For example, for the sake of this discussion, you decide on the “freezing” issue. The incident is the starting point of the investigation; therefore you need to select one object and one fault...ONLY

2. **Not being specific when gathering data** – You need to ask very specific questions

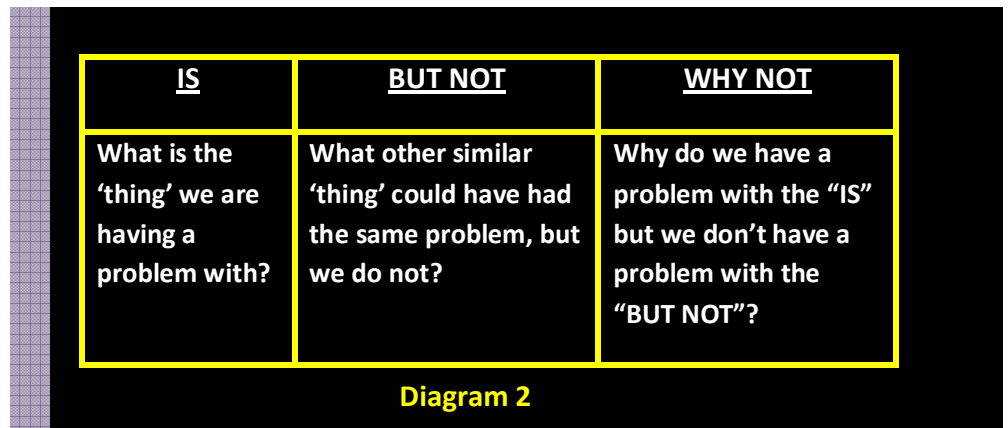
around that single object and single fault. Investigation teams are generally not very good as this, because they start with a poorly defined problem statement and too much data. In this case, let's take the SERVER as the single object which has a fault. Be as specific as possible with the exact server that has the fault, because you are dealing with a vast number of servers, both physical and virtual. In real life, it was a specific server called "ABC" and all users are working on this server for the same application.

Next, you need to look at a single fault, which is "freezing". Again, you ask the information source if they can be more

specific about the fault. In our example, it was reported that the server "is not communicating". When questioned, "What do you really mean by not communicating?" or: "Can you be more specific"? .... they determined that Server ABC was not "receiving packets".

So, this team refined its incident to be "The ABC Server using the RMC application was not receiving packets." This statement is quite different to the one they started off with, i.e., the server is freezing. They now have a much better chance of solving this incident quickly by narrowing the focus of their effort.

**3. Not consulting the correct information sources** – Another mistake that is often made by investigation teams is that the 'Data Base' team must solve the 'data base' problem or the 'Networks' team must solve the 'network' incident. Not true! At some stage during an investigation, the team of experts will exhaust their subject matter expertise. At this stage, they now need to look beyond themselves for answers. They now need



to get inputs from other SME's from where the incident could have originated. The first thing we do when we get involved with a client incident investigation is to change the faces around the table. You need to have your set of questions ready for the investigation and you need to ask "Who would be the best person to answer each question?" Many times, the best possible information source is outside your own silo or functional area of expertise.

**4. Not ring fencing data to create a contrast, elevating data to information** –What do we mean by "ring fencing" the incident data?

We mean that you need to seek what the incident could have been under these same circumstances, but for some unknown reason, is not. Imagine if you could do this for all the dimensions in Factor Analysis such as “What object, what fault, where/ location, which users, what time, what pattern, when in the procedure”. Such questions would read like

When in the procedure is the incident NOT occurring?”

Asking the “NOT” question is a powerful analytical intervention. It forces you to focus on relevant data and to eliminate the extraneous data. In our example of the “ABC Server Freezing”, the client asked the question “Which users are NOT experiencing the problem?” Initially, they did not know the answer, but when they involved the right information source, she surprisingly mentioned that it was only the users in the smaller outlets. That ring fenced the type of user very quickly. This was followed up with the geographic “Where” question and again they discovered new information... that it was only the smaller cities and not the bigger ones.

So, the scope of the investigation has been narrowed...it was only the smaller outlets in the smaller cities having the problem. This is drastically different from the original perception that the incidents were occurring nationwide. These realizations led them to the root cause very quickly. Ring fencing the problem by asking very specific “BUT NOT & WHY NOT” questions can lead to the realization of “new” information that will lead the team to the correct answer.

<u>IS</u>	<u>BUT NOT</u>	<u>WHY (NOT)</u>
Object		
Fault		
Users		
location		
Location of fault		
Date		
Pattern		
Stage of work		

**Diagram 3**

the following:

What other similar object(s) is NOT a problem?” What other faults are NOT occurring? Geographically where is the incident NOT seen? Which other users are NOT experiencing the incident? When is the incident NOT occurring? What patterns of occurrence are NOT happening?

**5. Not working with minimalistic information**

- One of the main reasons for incident investigation failure is “analysis paralysis”- having to work with too much data. In fact, so much data that they confuse the investigation team, hence the paralysis. Even with the most technical and sometimes seemingly unsolvable incident situation, we suggest to

the investigation team to only look at a maximum of 16 pieces of information. Once you've retrieved the accurate "IS" and "BUT NOT" information across the eight dimensions, as set out in Diagram 3, you will have enough information to find the technical reason why the incident occurred. These eight dimensions give you a snapshot of what the incident is and also what it could have been but for some reason, is not. All you have to do now is to find "WHY" or "WHY NOT".

**6. Not having a robust method for testing causal theories** – Replicating possible causes can take a long time, time which in most cases cannot be afforded. With the "IS & BUT NOT" architecture, it is possible now to "test" possible causes on paper before spending a great deal of unnecessary time and effort on each one. For a possible cause to qualify as a probable cause it needs to explain all 16 pieces of information in our fact gathering exercise.

**If "X" is the technical cause, then how does it explain we have a problem with the IS information and not the BUT NOT information?**

For a possible cause to be verified as one of the probable causes, it must be able to explain all the information in every incident dimension. If it fails to answer a single piece of information, logic dictates that it cannot be a probable cause.

Only when you are satisfied you have a reasonable, shortlist of probable causes, you can focus your time and effort to replicate these causes to confirm which one(s) is

actually the true cause. One of the more important benefits not mentioned yet is that all the stakeholders who worked through this investigation method in this structured way should agree on the true cause...no more unattended pet theories or minority reports.

### Summary

In summary, the benefits to the organization and its staff are the following:

- A common structured thinking approach utilizing the SME knowledge and experience of each member of the team.
- An approach to incident investigations providing visible feedback on progress and increased confidence in work done.
- An approach that is repeatable and user friendly for daily use.
- A set of worked questions to lead the investigator into asking the right questions at the right time.
- A proven process ensuring the identification of both true and root cause first time every time.

### Contact Details:

**Matthys J Fourie**

[Mat-thys@kepner-fourie.com](mailto:Mat-thys@kepner-fourie.com)

**+1703-946-1142 (USA)**