The Triangle of Information

In many areas of complexity analysis in systems people often don't gather enough data to be fully informed on the details of a problem or a fault. They can guess what the problem might be with a minimal amount of information, however if the information gather phase is extended to completion, then the problem or fault within the system or process often reveals itself rapidly.

Too many people do not gather enough data to sufficiently identify the exact details of an issue. They stop short and have to then gather more information as they iteratively change and test processes until success has been reached. That can be an expensive process. We suggest that it will be more cost effective to gather enough information to accurately know what a problem is. For, once the root cause of a fault or failure has been adequately described or defined then a solution can be found rapidly.

See the sequence of triangles shown below, they represent; reduction in possible failures, information gathering process, and identification of an accurate solution to a problem.

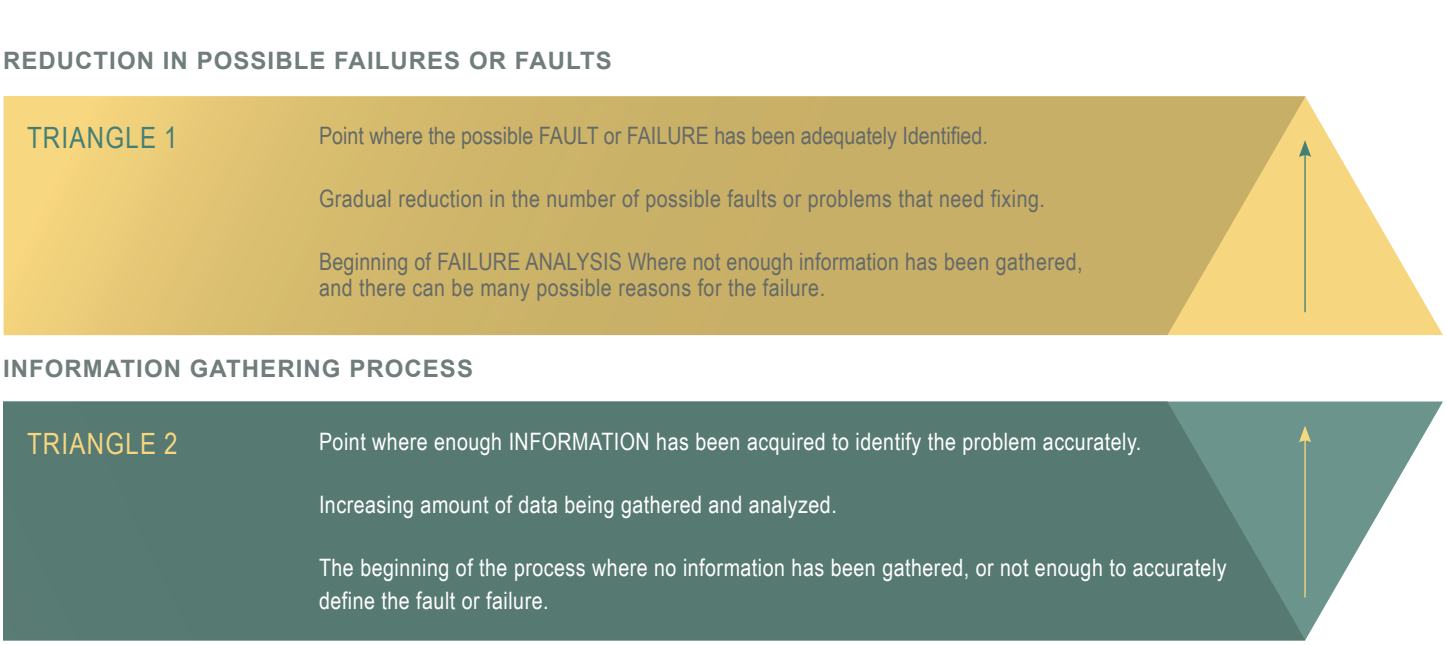

FIGURE 1

tools@ittimesavers.com

We can now overlay these triangles together and see how as we gather more data, we become more informed and eventually have enough information to know exactly what the problem or issue is, and hence the solution required. Often when individuals embark upon the failure analysis they stop too soon and then “try” a number of solutions until they get it right.

Of course, as part of the system checking and analysis after failure it is necessary to test various components of the overall system. However, the intention here must be as part of the overall information gathering phase and not a “hoped for” solution. [See Figure 2]

This approach to information gathering and problem solving is even more pertinent today as system complexity is increasing at an ever increasing rate. We can apply this to the world of IT and review threats through the lens of Cybersecurity Triangles of Information because one of the biggest challenges in IT Systems in 2020 is the management of complexity.

If we do not know what we have within our network how can we evaluate any cybersecurity threats? (We have not reached the 100% level of information gathered within the triangle) Therefore there maybe multiple threats that we are not aware of?

IDENTIFICATION OF ADEQUATE INFORMATION GATHERED AND SOLUTION RESOLUTION

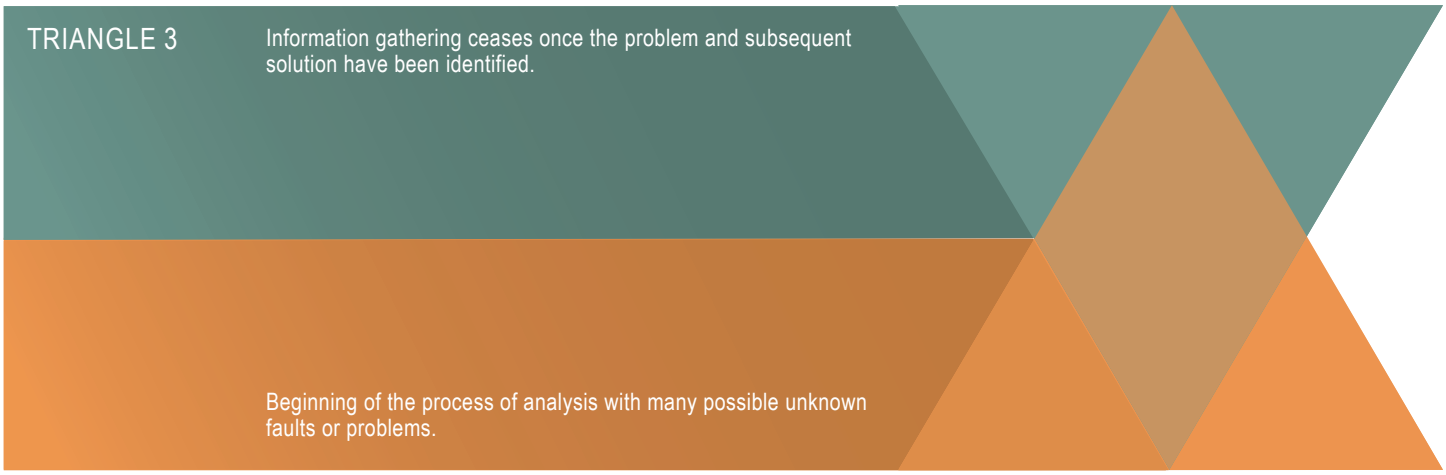

FIGURE 2

By applying the triangle of information model to IT systems and Cybersecurity we can logically identify possible threat levels by having all of the key data stored in the IT Time$aver Database tool. Once the data has been fully gathered for all of the devices (Blue Triangle) we can ascertain accurately what the threats could be. Without doing this type of incremental information gathering it is impossible for any company to be able to have an accurate picture of the the possible threats that may exist.

IDENTIFICATION OF ADEQUATE INFORMATION GATHERED AND SOLUTION RESOLUTION

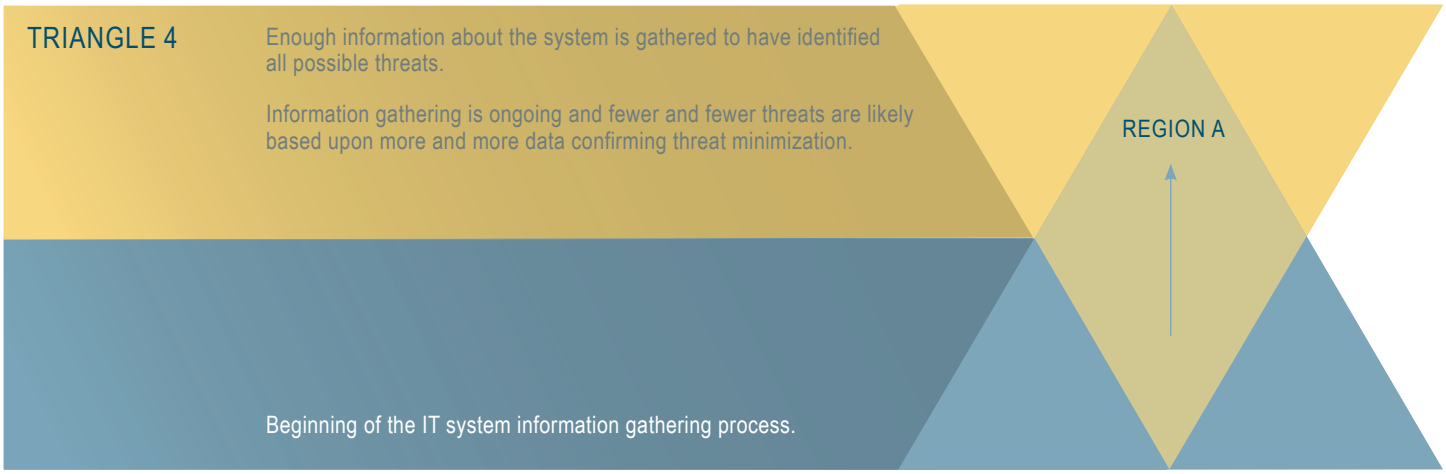

FIGURE 3

Region A

This is often the region of greatest vulnerability and greatest risk. The IT team have put time and effort into their cybersecurity risk mitigation process, but never quite finished it. However, they have the belief that what they have done is good enough. This is an illusion, for the bad actors in the cybersecurity world never sleep and continue to identify and exploit the holes that exit. It is a dynamic situation that demands constant vigilance as is shown by the cases of ransomware and DOS (Denial of Service) that are publicized on a regular basis. [See Figure 3]

TRIANGLE 5

INFORMATION GATHERED FOR AN IT SYSTEM

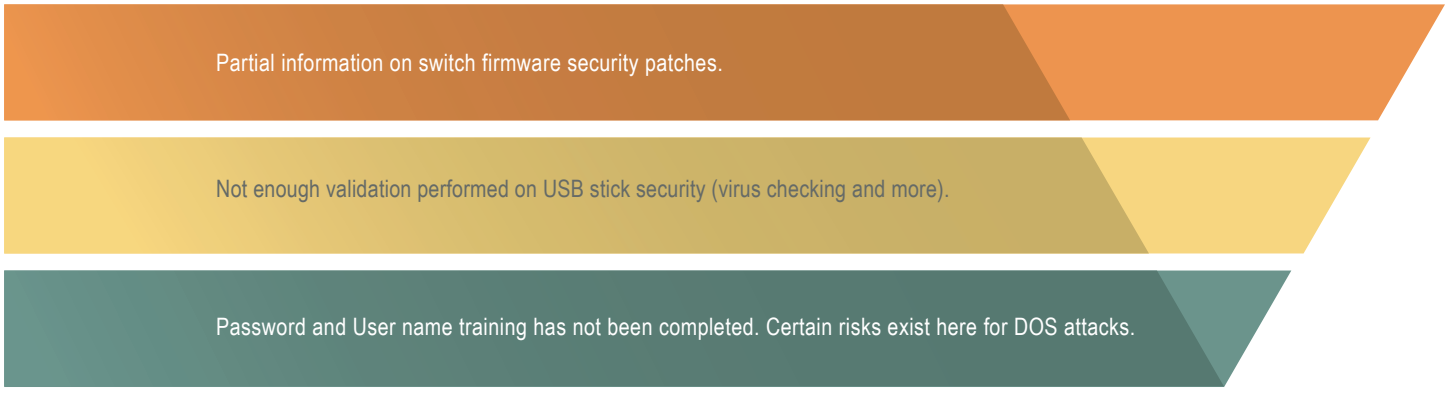

FIGURE 4