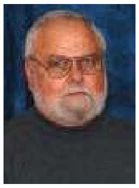
DITY™ Weekly Newsletter
itSM Solutions® IT Experience. Practical Solutions
The workable, practical guide to Do IT Yourself
Vol. 3.41 • October 16, 2007

The Incident Pit

By David Nichols



The "incident pit" is a slang term used by divers to describe a series of events, which by themselves would not normally be dangerous, but each causes a problem, which is made worse by the next event until you end up with a major incident. How many IT managers have found themselves at the bottom of an incident pit and didn't have a clue how they got there?

The whole idea behind the "incident pit" is that it's something that you fall into; it's never intentional, but it puts you in a situation where if anything else goes wrong the sides of the "pit" get progressively steeper.

In effect, the incident pit is akin to quicksand, but instead of sinking, you gradually fall into it. One small event leads to another, and the first thing you know is that you have one foot in the pit. Often you are not even aware of it until something else happens, and by the time you realize that something is seriously wrong the bottom is getting closer and closer.

Then, before you know it, you're at the bottom. A non-IT example of an incident pit is the loss of the USS Thresher; a leak caused an electrical fire, which in turn caused the nuclear reactor to shut down, followed by a failure to expedite its recovery, which left the ship with power which to continue to take on so much water that it unable to stop its decent and it passed below the sub's crush depth. Each event by itself was minor and recoverable, but the combination led to the loss of the ship and its crew.

Anyone who has been in IT for any meaningful length of time has been there. Incident pits are hard to get out of once you get into them, so it is best not to put "your foot in it." Let's take a look at what causes incidents in the first place, and what an IT organization can do to avoid stepping into the incident pit as they handle them. And then we'll look at the application of a technique developed during World War II and used in the healthcare industry that can be applied to helping us with how we handle incidents.

An analysis of diving accidents (a diver falling into the incident pit) revealed that there were four major causes:

1. Poor training
2. Lack of good judgment
3. Equipment failure
4. Lack of progressive experience

This is an uncanny description of the situation found in many IT service desks; that is little or no commitment to providing adequate training of first- or second-level incident control staff, coupled with management's failure to invest the time or effort to provide adequate training on the enterprise's business processes and how they impact the success of the company (this leads to a lack of situational awareness). The same can be said for over-investing in tools and under-investing in their proper implementation and use. Lastly is the common practice of using the service desk as the entry level "revolving door" to the IT department. Very little if any experiential knowledge is retained within the service desk or the incident control activity staffs.

There has been no shortage of news headlines where a company's IT infrastructure suffered from a major incident that significantly impacted its ability to provide its products or services for an extended period of time. Often the company explains it all away by letting the public know it was just a "little incident" that got out of hand.

Note that three of the four causes of incidents getting out of hand were due to poor training, lack of judgment and lack of experience.

ITIL's Incident Management process takes into consideration the need to have prepared, or "mapped in" to the normal Incident Management process, procedures to deal with major incidents. Those are incidents where time scales are collapsed and the organization must react with a greater sense of urgency. Incident Management staff are often formed into teams headed up by a dedicated "incident manager" who provides the direct supervision of the technical staff members involved in the restoration of the affected service. This avoids time and priority conflicts within the organization.

While bad things will always continue to happen to good people, and it is good to be prepared, it is also a good idea to look at those things that might keep your service desk staff (and you) out of the bottom of the incident pit.

Critical Incident Technique (CIT)

This technique, developed during World War II and subsequently published in the early 1950's, focuses on differentiating effective and ineffective work behaviors. It has been used to develop job requirements and develop effective professional practices. Its application for helping service desk staff avoid the incident pit is pretty straightforward.

The application of CIT relies on five major steps:

1. Structured incident review
2. Fact finding from the participants
3. Identification of the issues
4. Decisions to take affirmative action to resolve the issues
5. Evaluation of decision's probability of getting to the root cause

Structured Incident Review

Similar to ITIL's Problem Management's Major Problem Review activity, CIT depends on a structured (formal) review of a major incident. Information gathered during the review establishes the context (scope of the review) for the next area. The big deal here is that by making it mandatory to look at what happened sends a message to everyone involved that the organization is dedicated to finding out what went wrong and making sure it does not happen again. Just do not use it as an excuse for a witch hunt.

Fact Finding

It is important to talk to everyone who was involved in the incident. It is also important to do it quickly while everything is fresh in their minds. Document the facts through interviews, electronic and written records. Often the facts uncover hidden communication gaps or failure points in the Incident Management process itself. It is important to match the verbal record of events with event logs, or records from service desk tools and other enabling infrastructure management tools.

Identify the Issues

Once the Incident has been reviewed (scope established) and facts gathered, the next step analyzes the facts of the matter and the issues (causative factors) that contributed to the incident getting out of hand. This requires a significant amount of rigor to ensure that the causes are identified, not just the symptoms. This is not about placing blame.

Decision Making

At this point some decisions must be made to take affirmative action to prevent the recurrence of the events leading up to the major incident. Putting the participants through the effort to this point without some action to eliminate the process error or provide the required training to eliminate the potential of another occurrence is the worst possible outcome. By taking action to correct the issues it communicates a clear message that individual as well as organizational behavior will be changed in order to improve the overall process.

Evaluate the Decision

Similar to the Evaluation process in ITIL's Service Transition domain, the intent of this step is to evaluate the probability that the decisions made are likely to result in the desired outcome. It establishes a method of measuring the effectiveness of the outcomes achieved. It also helps overcome "group think" by holding up the decisions to rigorous evaluation.

Summary

CIT has been used effectively in several different industries, specifically in health care. It is particularly effective in separating major issues from minor ones. In effect it helps struggling organizations "cut out the noise" and focus on the really important issues. When those are resolved, the next more important issues can be addressed, and so on and so on. When applied to the Service Desk and the Incident Management process it can help organizations with dysfunctional processes to start getting a handle on things. It will help a good organization get better and a very good organization excel. It will turn the incident pit into something that other organizations fall into.