itSM Solutions® DITY™ Newsletter Reprint

This is a reprint of an itSM Solutions® DITY™ Newsletter. Our members receive our weekly DITY Newsletter, and have access to practical and often entertaining articles in our archives. DITY is the newsletter for IT professionals who want a workable, practical guide to implementing ITIL best practices -- without the hype.

become a member

(It's Free. Visit http://www.itsmsolutions.com/newsletters/DITY.htm)

Publisher
itSM Solutions™ LLC
31 South Talbert Blvd #295
Lexington, NC 27292
Phone (336) 510-2885
Fax (336) 798-6296

Find us on the web at: http://www.itsmsolutions.com.
To report errors please send a note to the editor, Hank Marquis at hank.marquis@itsmsolutions.com
For information on obtaining copies of this guide contact: sales@itsmsolutions.com

itSM Solutions®
IT Experience. Practical Solutions.

Vol. 2.49 DECEMBER 20, 2006

Fire Fighting is What You Want

DITY Weekly Reader

The workable, practical guide to Do IT Yourself

Many IT organizations think they are 'fighting fires', and that this is a bad thing. I disagree. I think its insanity, and that every IT organization and every person working in IT should strive to become more like firefighters.

hank
MARQUIS

Articles
E-mail
Bio

By Hank Marquis

Albert Einstein once said “The definition of insanity is doing the same thing over and over again and expecting different results”. Think about that quote for a moment and ask yourself if this applies to the way your IT organization operates.

Have you or your staff been fighting the same fires time and time again? Have you been doing the same thing over and over again expecting different results?

Many people equate “fighting fires” with being reactive and even chaotic. I have a different idea. It seems to me that reactive IT organizations are not “fighting fires”, because if they were they would be a well-oiled smoothly operating operation.

Think about fire fighters and what fire fighters really do:

- Team members from the various areas come together at the fire house, each knowing their role, duties, and position in the team
- They don’t quibble about who is going to drive the fire truck, or complain that they always have to open the door to the firehouse
- They assemble their tools, perform the required tasks, complete the mission, and then disband until required again
- They make every effort after putting out the fire to determine why and how it happened, uncover the root cause, and take steps to make sure it never happens again.

Chasing the same problems day after day is not fire fighting – its insanity. Many IT workers today have an attitude of “If It Ain’t Broke Then Don’t Fix It”, but if you are living Einstein’s definition of insanity than it is surely broken!

Based on my experience with many IT organizations, this article describes how Problem Management can help stop the insanity, and turn you and your team into real firefighters!

Root Cause Analysis

All IT outages occur from some combination of equipment, software and human error. ITIL Problem Management exists to establish root cause, examine proposed solutions, and to perform trend analysis.

What most miss is that the underlying root causes of most failures are often traceable to weak management; that is, procedures, programs and policies with errors or omissions. Such management weaknesses set the stage for failure and enable individuals to make mistakes. This is the real cause of most reactive organizational response to failures, incorrectly called “fire fighting” by many in IT.

Root causes are the most basic causes of an outage or failure event. Root causes have to meet the following conditions:

- They can be identified
- Management has control over them

Often for a single failure event there is more than one underlying root cause, yet most troubleshooters stop at the first root cause, which is usually the Configuration Item (CI) that failed or needs to change. This is **NOT** root cause. Root cause is the reason for the failure; not simply identification of the failed CI.

If the real root causes are not found and corrected, the underlying management weaknesses will lead to similar if not identical other failures—and this is the cause of the insanity within IT today.

For example, an IT organization claims not to have the time to perform preventative maintenance since they are so busy responding to failures. In this example, the failure symptoms (e.g., failing CI) are failing power supplies and other server components.

It is a failure of management to stop root-cause analysis after identifying which faulty component in the server to replace since the components will simply fail again without solving the true root-cause. Getting back to our example of failing server components, perhaps the true root cause is that the exhaust fan screens are clogged with dust; which limits airflow; which increases internal server temperatures; which causes components to go non-linear and fail.

A bit of management applied to the situation would try to determine the managerial (e.g., true) root cause of the physical root cause of the failure and remove it from the equation. Thus, the root cause is failure to perform preventative maintenance. If IT would vacuum the screens regularly, they would have fewer failures. The management root cause is failure to allocate and authorize resources to perform preventative maintenance. Without addressing this issue, the server will continue to experience regular failures.

Interestingly, most trapped in the endless loop of Einstein's insanity believe they don't have time to perform root cause analysis; yet they always have time and resource to fix a failure...

A Higher Standard

Root Cause Analysis (RCA) provides the means to determine how and why an event or failure happened. Understanding what happened, for example, that a power supply failed in the server is simply not enough. We also need to know why management allowed it to happen, and make no mistake, every failure is ultimately the result of some form of management error or omission.

Understanding what happened shows you the symptoms (e.g., failure physical root cause), but does not show you the underlying condition that requires correction (e.g., management control

root cause.) Failure events are just the symptoms of the underlying shortcomings of the administrative controls that are supposed to keep failures from happening in the first place. This is a very different thought process than that employed by most within IT today.

Failure to address the underlying management root cause simply sets the stage for the next physical failure event. Sound RCA is a deeper analysis of the underlying conditions to uncover and then correct those omissions that will contribute to future failures. Key features of RCA include:

- Understanding how a failure occurred; not just what occurred
- Discovering the underlying management weakness of the key contributors to the failure
- Developing and implementing practical and effective solutions for preventing future failures

While this may sound like what you are already doing, RCA is actually very different as experience shows that most technicians operate from intuition and assumption. One study shows that most technicians have jumped to an intuitive conclusion of what they plan to do, and formulate a strategy before they even finish reading the problem description! Key differences between RCA and traditional problem solving include:

- Reasoning through cause-effect instead of jumping to conclusions
- Focusing on facts versus supposition and intuition
- Considering a range of possibilities
- Thinking about procedural (management) failures vs. technical failures
- Discovering multiple root causes
- Trending data in order to discover systemic reasons for failure across more than one failure

Formal ITIL Problem Management include Problem Control (discovers root cause), Error Control (evaluates root cause data), Major Problem Review (deeper analysis of specific Problems), and Proactive Problem Management (trending.) These activities provide a very workable workflow and set of tasks that can easily help discover those management failures that keep IT staff “doing the same thing over and over again and expecting different results.”

RCA is not over until you have identified the management failure that allowed, enabled, or encouraged the hardware, software, or person failure. ITIL describes a Known Error as the root cause defined (e.g., what requires physically change to restore service), and a workaround established. I would like to add another requirement – documentation of what requires management change to prevent similar outages as well.

So consider adding another level of analysis to your existing troubleshooting—make an effort to discover the missing management control that set the stage for the physical root cause. After evaluating and trending a series of “management root causes” you will discover those key controls that you can easily implement to reduce future failures. Your reward will be true firefighting, and much more time to proactively eliminate even more physical and managerial root causes.

So, the next time someone tells you that fighting fires is a symptom of failing IT organization, tell them that’s insanity, and your goal is to be more like a fire fighter!

--

Where to go from here:

- Subscribe to our newsletter and get new skills delivered right to your Inbox, click here.
- Download this article in PDF format for use at your own convenience, click here.
- Browse back-issues of the DITY Newsletter, click here.

Related articles:

- "How To Measure IT Service Quality" by Hank Marquis for how to establish cost of downtime