

Effective Problem Solving

Root-cause analysis can identify solutions for data security breaches.

By Mark Hall and William M. Dickerson

A version of this article appeared in Biztech Magazine on 8/19/2009.

Since 2005, 255 million data security breaches involving sensitive personal information have been reported in the United States, according to Privacy Rights Clearinghouse.

When tackling the problem of data breaches, some rely on statistical analyses of industry trends. Information from actual breaches has been categorized by such criteria as business sector, type of data breached, and the proportion attributed to malicious acts, theft, hacking and careless or untrained employees. Solutions are then recommended based on the trend data exhibiting the highest percentages or greatest threats.

This approach is one of the reasons why problem solving is often ineffective: Solutions based on categories do not specifically address the causes of a given problem. Generic, categorical solutions fail at a much higher rate than do solutions targeted at specific causes of defined problems.

The problem management component of the IT Infrastructure Library framework sets the stage for an organization to adopt effective problem-solving strategies that will protect the company and its customers. Successful IT problem-solving organizations are increasingly implementing formal root-cause analysis (RCA) within their ITIL problem management structure.

Although there's a common perception that RCA is used to deal only with problems that have already occurred, it can also help to mitigate risk. RCA can be used to plan how a system or process should ideally function. IT can also enhance continuous improvement processes, demonstrate due diligence and analyze positive events so they can be repeated.

Using a multiple-event analysis, for instance, can help an organization find links between problems that might otherwise be undetectable using other tools.

Best practices when implementing RCA for IT problem management include:

1. Crafting threshold criteria based on business goals or scorecard metrics to identify incidents requiring full investigations.
2. Precisely defining major problems and quantifying business impact.
3. Allocating adequate time and resources commensurate with impact and risk.
4. Completing analysis consistently using the same process to ensure the RCA can stand up to independent auditing.
5. Instituting a rigorous validation process that uses evidence to verify causes.
6. Avoiding the creation of categories when analyzing problems and their causes.
7. Using the talents of the people who use, maintain and deliver IT services to help identify the best solutions. This is more effective than relying on an automated tool that uses formulaic solutions.
8. Prioritizing solutions based on criteria such as cost, payback and ease of implementation so they can be rationalized against business impact statements.

9. Developing solutions that are clear and descriptive enough to be successfully implemented by a third party and effectively monitored.
10. Focusing monitoring metrics on implementation timing and the effectiveness of the solutions, and reporting regularly on program successes.

About The Authors

Mark Hall is an account manager with Apollo Associated Services, a provider of root-cause analysis training, consulting, software and investigations.

William M. Dickerson leads the IT enterprise problem management group for a leading aerospace company.