REPORT - RCA ANALYSIS

RESPONSE TEAM ACTIVITY
Advanced Cybersecurity
Date: 09/05/24
By: Harshitaa Ashish – 21BCY10123

Summary

Root cause analysis (RCA) is a systematic strategy to determine the root cause of an incident by continuously asking "why" questions until no further diagnostic responses are available. It usually includes an analysis or a debate shortly after an occurrence occurs. A supplementary resource, the event state document, serves as a written record of what occurred prior to and during the incident, as well as responses to the questions required for a root cause investigation. The incident state document, also known as an incident report, is the appropriate place to begin the root cause analysis.

Introduction

Root Cause Analysis (RCA) is a broad word that refers to a variety of problem-solving techniques used to determine the root cause of a non-conformance or quality issue. Root Cause Analysis is the process of identifying, comprehending, and resolving an issue. The root cause can also be defined as the underlying or fundamental cause of a nonconformance, defect, or failure. Furthermore, the phrase "root cause" can refer to the specific point in the causal chain at which a remedial action or intervention would prevent nonconformance from occurring.

Objective

Root cause analysis tries to identify the difficulties that an organization should solve in order to streamline its processes and achieve its objectives. Identifying the root causes of a problem aids in the development of more effective problem-solving solutions.

Methodology

- The five "whys" method:

Ask a series of Whys. Why did this situation occur? Why did this happen...? Repeat several times until you find the root source of the problem. Ask a follow-up question to each why

question. Finally, the WHY will explain why the situation occurred. If we correct this issue, the problem will be solved.

- Change Analysis:

This method examines all changes to identify and establish a risk management strategy. This strategy is useful when there are multiple plausible causes. This includes thoroughly examining the changes that produce a certain event/problem.

- Cause & Effect Fishbone Diagram:

The Ishikawa Diagram is a visual representation of cause and effect. The problem is at the tail of the fish-bone picture, and each branch indicates a broad group of potential causes. This category, also known as clustered cause, is made up of sub-causes.

- Generate Solutions:

The cause and effect chart serves as a foundation for problem solving. We tackle issues by managing, changing, or eliminating their underlying causes. As a result, if the cause and effect chart effectively reflects the reasons of the problem, addressing those causes avoids future identical incidents (or significantly reduces their probability).
One prevalent fallacy is that all events have a single fundamental cause. This happens quite rarely. Robust solution strategies eliminate causes from various paths on the cause-and-effect graph. Diversification of solutions lowers the chance of recurrence compared to using single remedies.

- Produce the Final Report

Once the analysis is completed, we compile a final report. The final report serves as a communication vehicle for a larger audience, allowing others to identify and reduce hazards in their respective sectors. The report also serves as a 'lesson learned' record, allowing new knowledge to be shared with future employees.

Incident analysis

We begin by recognizing an occurrence, then study it to discover its features. The incident is frequently presented via an incident report, but there are other potential sources of information regarding the incident. For example, the RCA may be generated in response to a consumer complaint, a risk management referral, or even a complaint given by HR. Regardless of the source generated by the RCA, you must first identify the problem or incident.

Because there are so many RCAs issued as a result of incident reports, let's dig deeper. An incident report should contain the following:

- Administrative details.
- Incident information
- Eyewitness accounts and observations

- Actions and recommendations.

Incident sample case

Root cause statement: The Zoho Accounts servers were operational but unable to process any requests, causing Zoho CRM and Zoho Mail to have accessibility issues.
This availability event began on January 22, 2019, at 15:31 IST and terminated at 15:52 IST. Site24x7 noticed the problem, which affected the Zoho CRM and Zoho Mail services.

Response

Customers reported the situation, and the incident coordinators from the Zoho CRM and Zoho Mail teams responded by contacting the incident manager and involving product team chiefs and other stakeholders. The event was addressed within 15 minutes of its occurrence, and a temporary solution was offered.

Impact analysis

The delay lasted 21 minutes, and Zoho CRM and Zoho Mail clients were unable to access their services. Following the incident, 20 support tickets were raised by phone, email, and live chat.

Results

The former user interface included the ability to sort services. The listing was no longer required, thus we deleted it from the codebase.

We also found and eliminated related functions that use the same sorting technique to prevent this downtime in the future.

Root cause analysis

Root Cause Analysis (RCA) is typically a step in a wider problem-solving process. A Root Cause Analysis can be conducted using a variety of tools. Some of them can be done by a single individual, but in most circumstances, a Cross Functional Team (CFT) approach will yield the most benefits and maximize the odds of determining the underlying "root cause".

Several problem-solving methodologies, like the Eight Disciplines of Problem Solving (8D), Six Sigma / DMAIC, and Kaizen, incorporate Root Cause Analysis into their methodology.

Implementation

The key to a successful root cause analysis is a thorough understanding of the situation. Root cause analysis (RCA) is an analytical method that assists you and your team in determining the root cause of a problem. RCA can be used to investigate and correct the underlying causes of repetitive incidents, major accidents, human errors, safety near-misses, quality issues, equipment failures, medical errors, production issues, manufacturing errors, delivery delays, and environmental releases, as well as to identify potential issues ahead of time.

Understanding a working process or sequence is critical for successful root cause analysis. The event is the cause of the effect. A cause is a combination of circumstances or factors that enable or facilitate the existence of a condition or event. As a result, the most effective technique would be to investigate why the occurrence occurred. Simply simply, removing the cause(s) will erase the effect.

Mitigation

The information in the incident state document serves as the foundation for conducting RCA. The incident manager determines the departments and processes involved in CAPA and conducts a thorough investigation. Throughout the RCA process, we learn lessons and identify areas for improvement.

Corrective measures are predicated on a previous unpleasant experience. Preventive activities are designed to thwart a bad event in the future. Corrective Action Preventive Actions, also known as CAPA, are critical components of our continuous improvement approach.

The success of RCA depends on thorough monitoring of the action plan. So the next step in the RCA process is to develop a proposed action plan that outlines a list of corrective and preventive activities. The action plan should specify the timeline for completing the actions as well as who will be in charge of each job.

Conclusion

Using an incident report as the foundation for a root cause investigation is logical from a safety process standpoint. However, depending on the industry, it may be rejected. Take the medical industry as an example. Every day, many hospitals get hundreds, if not thousands, of incident reports.
The truth is that as industry leaders, we all need a framework in place for categorizing issues by priority level and, as a result, resolving the deluge of incidents. If the most severe cases are triaged to a root cause analysis, there may still be hope for an effective reporting system.