INCIDENT MANAGEMENT VS PROBLEM MANAGEMENT: DIFFERENCES EXPLAINED

In this article, we're explaining the differences between incident management and problem management.

First, I'll start with a recent event that shows how service providers can successfully perform both incident and problem management.

The UK Network Rail power surge

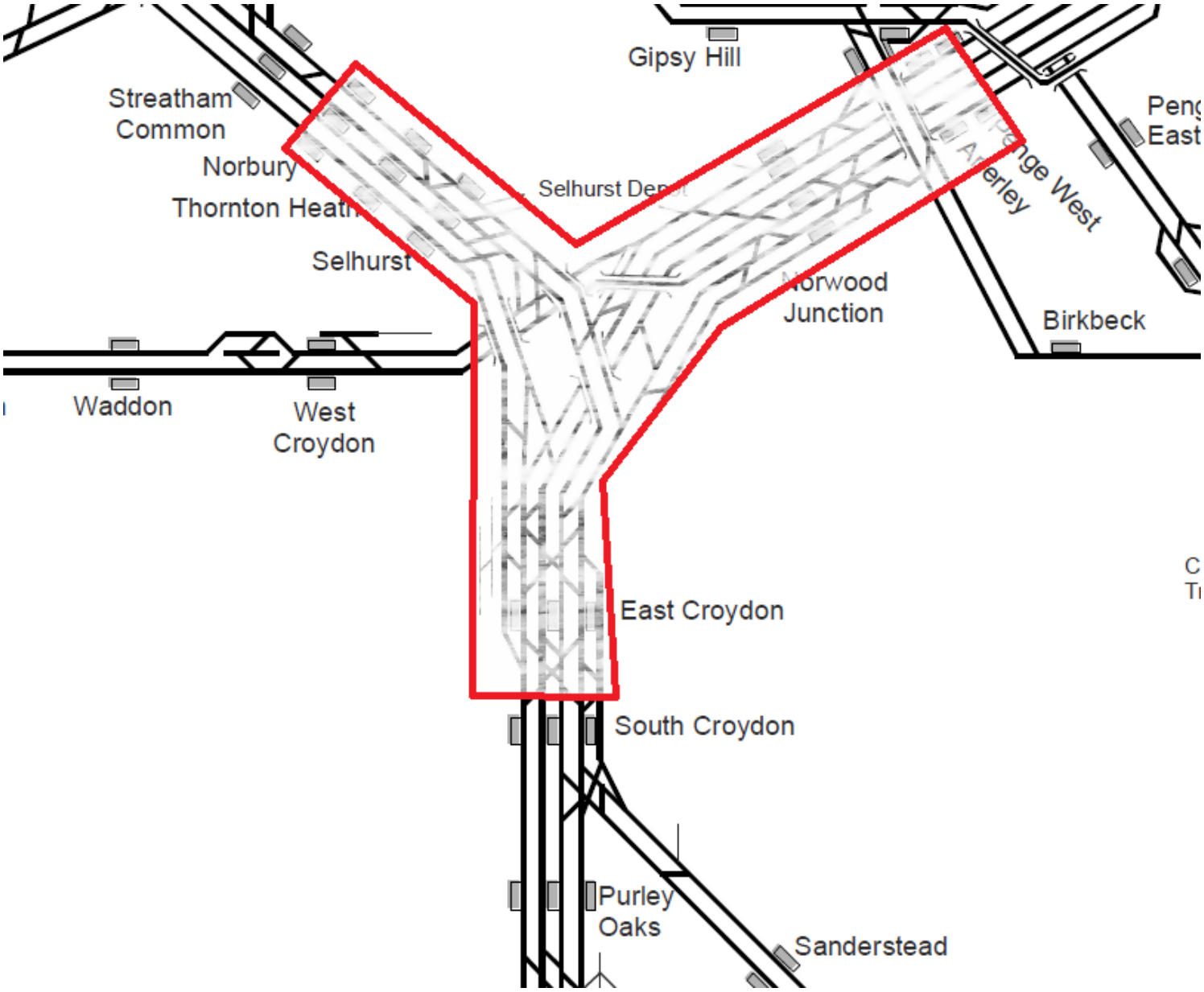
On December 19, 2019, the United Kingdom's Network Rail sent out a series of tweets detailing a signalling control issue that halted rail services the previous day for over an hour. The Southern Rail, which handles over 7,000 passenger and freight services daily, experienced a 20-second power surge that knocked out four signalling control stations at one of their busiest sections.

Technicians were sent to manually reset systems that automatically shut down in order to protect from any surge damage. Backup power supplies never kicked in because there was still power, and UPS systems provided no surge protection.

(Network Rail continues to investigate how to prevent such a surge from impacting the systems in the future.)

The tweets and subsequent website post have received acclaim from many people. Affected

customers in particular praised Network Rail's clear apology, the candid explanation of what happened, and their next steps in investigating and preventing recurrence.



In IT service management, it's inevitable that you'll deal with issues such as:

- Outages
- Performance degradation
- Data breaches

The way you handle these issues determines, to a large extent, how customers and other stakeholders perceive your company, as a service provider. This is where two vital ITSM practices, incident management and problem management, come into play.

Of course, users and the business are interested in quality services, not terminologies. Understanding the value of the two practices in handling issues affecting services is your responsibility as the service provider.

What is incident management?

To understand incident management, let's start with the incident. The ISO/IEC 20000:2018 service

management standard defines an incident as any of the following:

- An unplanned interruption to a service
- A reduction in the quality of a service
- An event that has not yet impacted the service to the customer or user

The purpose of incident management, according to ITIL 4, is:

> *"To minimize the negative impact of incidents by restoring normal service operation as quickly as possible."*

Just like the Network Rail outage example, most incidents have a direct impact on customers and users. That's why speed is the most important thing in incident management—the priority is the return to normal service delivery.

For Network Rail, sending technicians to manually reset switches after remote action failed is a clear example of speedy response. (It's also the classic "turning it off and on" approach!)

Lifecycle approach to incident management

In service management, most incidents are managed in a lifecycle approach that involves logging, categorization, prioritization, escalation, resolution, and closure.

- **Logging, categorization and prioritization** determine the right course of action, including who should handle the resolution, the extent of communication, and the speed of response. A major incident would be one which has significant impact and urgency, requiring an all-hands-on-deck approach.
- **Escalation** functions across higher-level specialist teams, vendors with better capabilities to address the incident, and higher manager levels that can make the necessary decisions about communicating to shareholders and regulators and approving emergency changes or necessary resource allocation.
- **Resolution** can be done by the user through self-service, handled by the service desk or support teams, or invoke disaster recovery measures.
- **Closure** involves talking with users to confirm they are satisfied that normal service has resumed.

Handling incidents successfully requires significant communication and collaboration.

- Techniques such as swarming are key in bringing stakeholders together to diagnose and determine the most appropriate ways and people to resolve the incident.
- Communication during and immediately after the incident also provides relief to users and stakeholders—assuring your users that the incident is being treated with the level of seriousness it deserves, be it big or small.

Afterwards, an incident postmortem documents what we learned and identifies paths forward after similar incidents that may occur in the future.

(Learn how to run incident drills and map the incident management process.)

What is problem management?

A problem is defined by ISO/IEC 20000:2018 as:

"A cause of one or more actual or potential incidents".

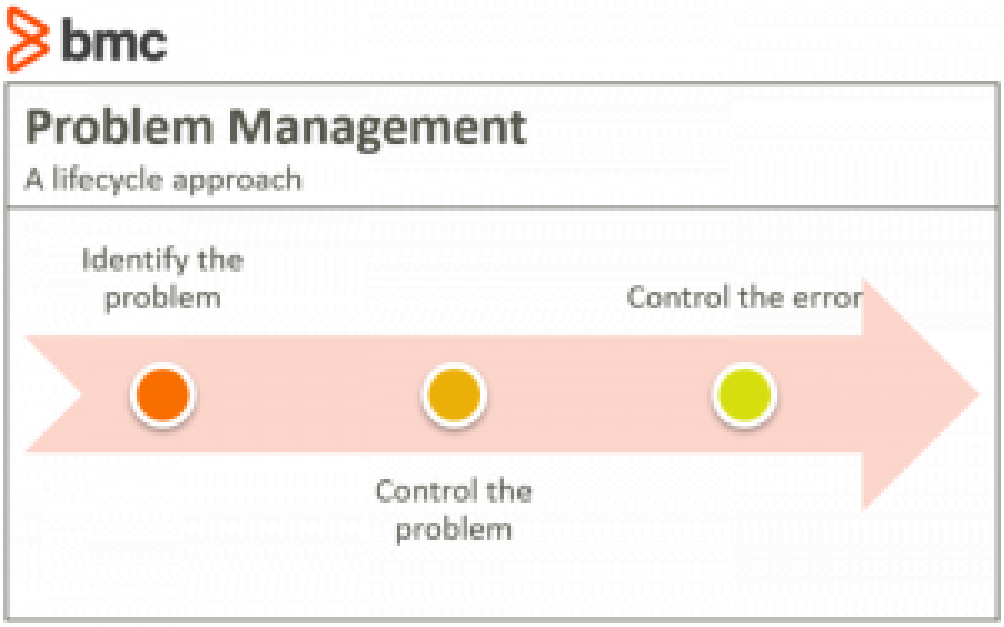
According to ITIL 4, the purpose of problem management is to "reduce the likelihood and impact of incidents by identifying actual and potential causes of incidents, and managing workarounds and known errors."

In problem management, the focus is on the future, identifying and controlling problems, so thoroughness—not speed—is the emphasis.

The Network Rail Investigation into surge effects on signalling and power supply equipment after the switches were reset and service resumed is a perfect example of problem management. The Network Rail could have resumed service (incident management) and stopped there, choosing not to work on long-term improvements (problem management).

Lifecycle approach to problem management

Like incident management, you can handle problem management with a lifecycle approach. The main activities in the problem management lifecycle are:



- **Problem identification,** including logging, categorization, and prioritization
- **Problem control,** such as analysing and documenting workarounds and known errors
- **Error control,** including fixing errors through change control and assessing effectiveness of workarounds

Techniques to identify root causes of incidents are varied in number and range from simple, like brainstorming and 5 Whys, to more complex methods, like the Kepner-Tregoe Method and Ishikawa Diagrams.

Reviews of problem management activities can be done as part of sprint retrospectives, change planning, and vendor meetings.

The value of problem management

All service providers have existing relationships to their incident management as well as their problem management, whether you're proactive or reactive. Problem management is arguably more valuable due to its focus on preventing recurrence or limiting impact.

Unfortunately, due to its background nature—we don't see what we have prevented—it is overshadowed by the more heroic incident management, with customers directly feeling its impact.

The fire fighters and emergency response teams get the glory for saving the day. The detectives and forensic investigators who perform painstakingly long investigations are rarely showered in accolades because customers will not feel the impact of future incidents.

I feel that service provider leadership should pay more attention to problem management efforts, particularly through two methods:

- Reward structures
- Communication

Documentation and automation of workarounds is one way in technical teams can spend more time investigating root causes, and rewards should focus on those efforts. Similarly, reporting on a similar incident that passed with limited impact after problem control measures were enacted will go a long way in reassuring stakeholders that valuable work takes place post-incidents.

Related reading

- BMC Service Management Blog
- The Role of Incident Commander (IC)
- The State of Incident Management