Network and Service Outage Analysis

Introduction

A network or service outage is the loss of network resources including routers, switches and transport facilities, predominantly because:

- There is a complete or partial failure of hardware and software components;
- Power outages;
- Scheduled maintenance issues;
- Operational errors such as configuration errors;
- Acts of nature such as floods etc.
- Unforeseen damage to infrastructure e.g. fibre breaks or third-party damage.

According to research carried out by CISCO in the USA:

- **23%** of outages are caused by router failure;
- **32%** for link failures (fibre breaks);
- **36%** following failed maintenance programmes;
- **9%** for other miscellaneous reasons.

Focus on these can result in reductions across the board through engineering out the faults. However, there are two elements to Service Outages – Engineering and the processes or otherwise that delay restoration of service.

Better management by Design

The MCW Service Outage Analysis is a tool for forward thinking organisations to both analyse a recent major service Outage or incident and inform programme of continuous improvement. This analysis is an important deep dive that avoids the allocation of blame but is part of a portfolio of initiatives to address failings in Service management.

After Service failings management is keen to assure stakeholders that they have control of the situation and will rush to judgement as to root cause and a long-term fix. The MCW SOA will address the elements of any outage including:

- Reducing the frequency and duration of outages;
- Improving Mean Time to Repair (MTTR);
- Facilitating the smooth management of critical outages;
- Eliminating inhibitors to good service management.

The output of the MCW SOA is clear exposure of the risk of future outages, as well as recommendations for improvement. MCW works with you, your partners and customers. We examine past outages, related change and configuration artefacts and importantly we review the impact on both your organisation, service models and infrastructure on availability.

What are Inhibitors?

Research reveals that teams that adopt the traits and habits of high performing professionals, and eliminate poor habits manage major incidents significantly more successfully than those teams that do not. The major inhibitors to successful management of major incidents are:

I. **Poor Process:** Slow delivery of process, in decision and/or poor process design;
II. **Management Behaviour**: The transmission of heightened tension, or even displays of temper will have a debilitating impact on the team;
III. **Business Culture:** Blame cultures, Businesses that are strictly hierarchical and allow no room for initiative, businesses where employees are under constant and unrelenting pressure. Customer organisations prone to blame suppliers, Service Providers prone to blame customers;
IV. **Poor Resource Deployment**: Insufficient or poorly located resources.

The SOA delivers change

Making Change Work is what we are all about by delivering a holistic analysis, that delivers a 'warts and all' assessment of the Service Outage(s) that you wish us to analyse, in a blame free environment, designed to create a roadmap to improvement. It can also be used when faced with a party determined to unreasonably allocate blame to your organisation and you wish to determine what the evidence supports. The Project involves:

- collecting outage data,
- interviewing those involved in managing the outage;
- Interviewing the service personnel who resolved the outage;
- Understanding your business culture;
- Observing and analysing your management styles.

We then analyse the data:

a. Creating groupings and classification to ascertain whether the impact on the outage was "significant" or "less significant." We focus only on those labelled "significant"; and list the "less significant" for future action;
b. For each "significant" outage, review the root cause. For example, faulty hardware or software. This is probably already known since the outage is resolved;
c. Using a Pareto analysis (80/20 rule), we rank the related causes. You will see that most of the outages result from a range of causes not simply faulty hardware or software or poor response;
d. We examine the reasons for the duration of the unavailability. For example, the outage may have occurred because of faulty hardware or software; but the duration of the unavailability might have been extended by lack of tools, management behaviour, business culture, training, spares, etc.

e. We review and analyse:

- Existing procedures and support policies that were invoked or used during this outage; The actions (or inactions) of staff members, customers and anyone else involved in the outage or restoration;
- Anything that might have lessened the duration of the outage or avoided it altogether. The examination should locate a trend, or at least something in common with similar outages. This is what you are looking for - the "smoking gun." Then we quantify the avoidable outage time.

An Actionable Report

MCW will prepare a report with recommendations for change to address the most significant generators of preventable downtime. The end of the SOA is the creation of a report providing:

- An Executive summary of findings;
- Fault Fix Time Line;
- Problem/Fault management Reports;
- Technical Fix Description;
- Description of Risks and Issues;
- Recommendations and Observations.