BCP/DRP CASE STUDY: ADAPTING MAJOR INCIDENT HANDLING RESPONSE FRAMEWORKS TO A CORPORATE ENVIRONMENT

Pieter Blaauw

Pick 'n Pay Information Systems
pblaauw@pnp.co.za

ABSTRACT

Business continuity is defined as "The degree to which an organization may achieve uninterrupted stability of systems and operational procedures during and after a disruptive event". Business continuity and disaster recovery plans and the very need for them became to a frightening reality after September 11 2001. Never was the emphasis on disaster recovery and business continuity placed so heavily on business following a world event, and it has shaped how modern business approach these two interwoven aspects of their business.

Fortunately not every business suffers a major disaster in its lifetime. On the contrary, many businesses today, large or small, face what can better be described as challenges, but these can have far reaching effects on the bottom line. The need for incident handling frameworks in business has thus come to light, and this paper will look at how one corporate in South Africa has adapted a major incident handling framework to their unique environment, with the hope that it can shed some light for other corporations to adapt to disruptive events in their business. The paper will cover severity levels, minor incidents, major incidents and the processes followed in the incident handling framework.

KEYWORDS

Major Incident Handling, Minor Incidents, Major Incidents

BCP/DRP CASE STUDY: ADAPTING MAJOR INCIDENT HANDLING RESPONSE FRAMEWORKS TO A CORPORATE ENVIRONMENT

1 INCIDENT MANAGEMENT

An incident is any event that disrupts a companies normal operations, no matter how small. Incidents happen on a daily basis across companies but the majority of these incidents have a very low impact. Nevertheless all incidents need to be managed properly to ensure that the effect on the company is minimized. Incident handling is not simply a technical function either. Policies and procedures need to be in place prior to the incident(s) taking place.

1.1 Incident classification

There are several ways that companies classify incidents and their severity levels. Some companies use the red, orange and green systems, others use a numerical system. Within Pick 'n Pay Information Systems, a numerical system is used, where the incident is classified depending on its severity and impact on the company, with a severity level 1 being only a notification of a possible problem, and a severity level 4 being a major system or service outage.

This numerical system does serve as a guide only and each incident is dealt with based on it's impact on the organization and not the underlying Service Level Agreement or business process. This ensures that incidents are escalated quickly and gives the organization time to react to the incident should the severity of it require such action.

	Routine Incident
Severity 1	Routine Daily Issue Zero or Minor Business Impact Localized scope, closed within a few hours
	Significant Incident
Severity 2	Service degradation or Outage. Impact to several users. Escalation of issue longer than a business day.
	Serious incident
Severity 3	Serious service degradation or outage affecting a entire line of business
	Severe Incident
Severity 4	Severe outage affecting one or multiple areas of business Threat to actual loss of reputation, trading loss, and or settlement impact. Requires senior management control

1.2 Minor Incidents

Minor incidents occur on a regular basis. On their own they cause minimal disruption to the company. However, there needs to be an appropriate response to them since they can have a far reaching impact if not checked.

1.3 Major Incidents

As incidents increase in severity, and as such their impact on the company, so the response to them should similarly increase. Routine and Minor incidents usually have a fairly standard response, according to the policies and procedures of the company, and more severe incidents are handled by enhancing the standard business arrangements.

The most severe incidents (Severity 4 in our table) i.e. those affecting the widest area in business, requires a more structured incident handling process more complicated than the normal business processes, referred to as a Major Incident Handling Framework.

2 MAJOR INCIDENT HANDLING

2.1 Process

Major Incident Handling frameworks are management structures applied to the response plans and arrangements for the most severe incidents in a business. The precise structure and response procedures varies from business to business, and also from business unit to business unit. However, in any other company, like Pick 'n Pay, the objective of these procedures remains the same, to ensure there is an effective and appropriate response to all major incidents that can affect the business.

Business units in any company, like Pick 'n Pay, have different priorities and business drivers. It stands to reason that because of this, each unit's MIH process will vary according to their circumstances and priorities. There are some shared features and roles in every MIH, no matter where it is applied and what the company may be.

Incident Owner: The individual or business unit responsible for the resolution of the incident in the business. If the resolution lies outside the company, in this case, Pick 'n Pay, it lies with the management responsible for the SLA with the outside solution provider.

Communications: In any event or incident, communication is crucial in the handling of the event. In a major incident handing framework it provides for the accurate and timely communication of information to all the affected parties inside and outside of the business. Communication provides those with a role in the incident handling procedures with all the information they require and relieves those who are dealing with the incident with having to provide the rest of the organization with information they require.

Technical Recovery: Where the cause of the incident is within the organization, it's important that it gets resolved within the organization. Technical recovery relates to the underlying technical issues and persons involved in recovering from the incident.

Business Recovery: A major incident will disrupt the organization's business. The extent of the interruption may be sufficient to warrant the implement and certain plans and arrangements to manage the disruption in order to ensure that critical business processes are maintained as far as possible during the disruption.

Due to the differences in organizations the way that these procedures happen varies from company to company. The following activities needs to be covered in each process though.

Assessment: Once an incident has occurred it needs to be assessed in terms of its impact on the company and its operations and business processes. A severity level will then be assigned to the incident and the severity level then determines the response to the incident. An important aspect to keep in consideration is that a incident's severity level can change during its life.

Warm-up: If an incident has been classed as a Severity 3 or 4, and it has been determined that the full MIH process needs to be invoked, a warm-up period is required. This is to assemble the required team and assign the correct roles to each member of that team.

Incident Management Cycle: Once a MIH process has been established, it will consist of a set of procedures that will repeat itself through a cycle. How often and when the cycle repeats itself depends on the incident and the organization.

Assessment: Asses the situation and device a plan

Activities: Implement the plan

Review: Look at the action to determine if the plan was able to resolve the situation

Communication: Update those involved in the previously defined steps / plan

Cool Down: Once the incident has been resolved it is necessary to stand down the MIH process. This means communicating with all the involved parties that the incident has been resolved.

Post Incident Review: On severity 4 incidents its recommended that a Post Incident Review take place to establish what the cause was and how corrective actions can be put in place to prevent a repeat of similar incidents.

3 WATCH STATES

Watch States are used in MIH to heighten awareness in three situations

There is a reason to believe that an incident may occur

There is a reason to believe that an incident which has occurred may escalate further

An incident that has occurred has not been fully closed

The purpose of a Watch State is to monitor the situation closely and facilitate the response and escalation to the next level. When a watch state is declared, consideration needs to be given to:
Who should be advised of the situation
Who should be advised that they may required to respond to the situation
Preparations that need to be carried out to deal with a possible escalation

Once an incident has been declared and the use of the Watch List implemented it needs to be reviewed on a ongoing basis. The nature of the incident will determine how often. As an example, in Pick 'n Pay, a Point of Sale incident will be reviewed far more frequently than a e-mail incident, due to the very nature of the business and the affect it has on the business.

4 INCIDENT ESCALATION

As seen from the previous sections, of the paper, an incident can be classified at any one of the four levels of severity. During the MIH process the incident can then be escalated to another level as deemed necessary. While in theory the incident owner should be responsible for escalating (and de-escalating) the incident between levels, in Pick 'n Pay a single problem manager is responsible for this task, and consults with various people before taking the necessary action.

By using a Major Incident Handling framework, making these decisions with the aid of the BCM or BCC and other stakeholders, and defining actions that need to be taken becomes that much easier and simpler.

5 POST INCIDENT REVIEW

Incidents represent a disruption to any company's normal operations. It is therefore in the company’s best interest to minimize the number of incidents and their severity. It stands to reason that after every severity 3 or 4 a Post Incident Review needs to take place to identify the cause of the incident and if possible, take action to reduce the chances and risk of the incident repeating itself.

The extent of the review will be determined by the extent of the severity and the affect it had on the business. For small severity 1 and 2 incident just recording the time and incident may be enough. Should there be a small number of the same incidents it can identify a trend which could then allow for corrective action to be taken.

For more severe incidents (especially severity 4), for example a Point of Sale failure, a more in-depth review needs to take place, to identify the underlying cause. If possible this cause should then be addressed to prevent a possible repeat of the incident.

6 REFERENCES

EPT Consulting (http://www.etpconsulting.co.uk/Business%20Continuity/business¬continuity-glossary.htm)

Rittinghouse & Ransome, Business Continuity and Disaster Recovery for Infosec Managers, 2005

Hunton, Bryant & Bagranoff, Core Concepts of Information Technology Auditing, 2004