



Steering Committee

2B

Update on the MSRC Work

March 14th 2011

Current Events/Status

- ❑ 2B has completed it's work
- ❑ Four 50+ page documents were reviewed and updated.
- ❑ Radio, Television, DTH, CATV and MVDS systems.
- ❑ In MSRC I, a number of best practices were created.
- ❑ During the time between MSRC I and II it was found that because the best practices were written at the 50,000 foot level they did not translate well into actionable items for the local engineering and operating personnel.
- ❑ MSRC II Tool Kit working group turned those best practices into a sample manual on how to set up a disaster recovery plan and a self assessment checklist on the preparedness of a facility.

Vulnerability Checklist

Does a Disaster Recovery Plan exist that details how to effectively assess impact to the facilities and recovery operations in the event of an emergency?

- Yes
- No

Does the Disaster Recovery Plan identify essential personnel necessary to carry out restoration efforts?

- Yes
- No

Does the Disaster Recovery Plan describe the Recovery Time Objective (RTO) to establish the backup origination facility in the event of an emergency and for how long the backup origination can be sustained?

- Yes
- No

Comments:

- We made numerous small formatting changes.
- We changed several references to the words “Mandatory” and “Required” to “Encouraged” or “Recommended”
- This was done in all the documents.
- These are best practice documents.
- DRP should be reviewed annually. It may not be beneficial to test all elements annually

Comments:

- ❑ Cable document
 - ❑ No direct mention of the 2 way services that cable systems provide today
- ❑ The focus is on the restoration of “service”, making no distinction what services.

Next Steps

- ❑ These documents, as updated, will be useful to the local engineering and operational personnel of the various industries.
- ❑ They should be widely circulated to those industries to be used as templates for their various disaster recovery scenarios.
- ❑ At a minimum, the vulnerability checklists should be reviewed at the local level of the various entities that these documents target.