Revolution Capital Management

Business Continuity and Disaster Recovery Plan

Revision History

- January 23, 2012: Updated with latest information
- January 18, 2011: Updated with latest information
- January 17, 2010: Updated with latest information
- March 2, 2009: Updated with latest information
- January 8, 2008: Updated with latest information
- August 14, 2007: Initial PowerPoint version

Contents

- Redundant Operational Facilities
- Document and Data Backups
- Critical Staff Competencies
- Third-Party Failures
- Disaster-related Communication Plan
- Testing and Updating the Plan
- Specific Risk Factors and Mitigation Plans

Redundant Operational Facilities

- Operational Facility #1
  - Located at Earthnet in Boulder CO.
  - Redundant server operates on an uninterruptible power supply (UPS).
  - The site also has its own diesel generator to guard against long-term power outages.
  - The facility uses multiple internet providers.
  - Earthnet has access to 2 separate power grids and has automatic failover from grid to grid.
- Operational Facility #2
  - Located at the RCM main office.
  - Redundant server operates on a UPS.
  - This facility is geographically separate from facilities #1 and #3 and is on a different power grid. It also uses a separate internet provider.
- Operational Facility #3
  - Located at Rob Olson's residence.
  - Redundant server operates on a UPS.
  - This facility is geographically separate from facilities #1 and #2 and is on a different power grid. It uses Qwest/Earthnet as Internet providers.

REVOLUTION Capital Management

Document and Data backups

- Documents
  - Critical hard-copy documents are stored at the main office (in a locked enclosure).
  - Critical electronic documents (both originals and also copies of hard documents) are stored on a secure, remote, commercial site using a RAID5/6 array (www.codesion.com).
  - DVD copies of copies of documents are made periodically.
  - Backup status is reviewed and maintained at least once per month, and more frequently as necessary.
- Data
  - Data is stored at the main office on a RAID6 array.
  - Data is also archived on a RAID1 array at a location distinct from the main office.

Critical Staff Competencies

- Understanding of model signal generation
  - All three principals possess this competency.
- Knowledge of FCM and executing broker and associated contact information
  - All three principals possess this competency.
- Knowledge of data provider and associated contact information
  - All three principals possess this competency.
- Knowledge of hardware infrastructure and ability to address hardware-related issues
  - All three principals possess this competency.

Third-Party Failures

- A second-source data provider is in place in order to provide a backup source. The current primary data source provides the daily updates via FTP.
- Alternate trading desks can be used in the event of issues experienced by our primary trading desk. Our primary IB, FCI, has access to alternate desks.

Disaster-related communication plan

- There are currently two (2) employees to contact.
- The three managing members and two employees will contact each other in person, via telephone, or via electronic mail/messaging.
- Data vendors will be contacted, if possible, via telephone or electronic mail.
- Brokers and trading desks will be contacted, if possible, via telephone or electronic mail.
- A full contact list is maintained by each of the key personnel.

Testing and updating the plan

- How often is the plan reviewed?
  - The plan is reviewed at least on an annual basis.
- How is the plan tested?
  - Testable components of the plan are tested via normal operational contingencies.
- Where are plan copies maintained?
  - Plan copies are maintained at the main office, at the residences of each of the managing members, and on a remote server.
- Who has received the plan? How does one ensure that those who 'need to know' do receive the plan?
  - All managing members and employees have received and are familiar with the plan.
- Do we have NFA emergency contact information?
  - NY office: (212) 608 8660
  - Chicago office: (312) 781 1300
  - Information center: (312) 781 1410 or (800) 621 3570

REVOLUTION Capital Management

Specific Risk Factors and Mitigation Plans

Risk Factor #1

- Failure type: Hardware failure with signal-generating servers
- Impact: Inability to place orders or modify positions
- Severity level: High
- Mitigation: Independent local servers, co-located remote server, RAID 5/6 protocols used to ensure data integrity, software copies stored in a remote, commercial repository, failover plan in case primary server fails.

Risk Factor #2

- Failure type: Software failure with signal-generating servers
- Impact: Inability to place orders or modify positions
- Severity level: High
- Mitigation: Extensive testing before deployment, daily monitoring of systems to ensure presence and validity of orders

Risk Factor #3

- Failure type: Market data receipt failure
- Impact: Inability to place orders or modify positions
- Severity level: High
- Mitigation: Data sent via multiple methods (email and FTP), end-of-day price data can be obtained manually from exchange websites, second data source.

Risk Factor #4

- Failure type: Short-term power outage (2 hours or less)
- Impact: Inability to place orders or modify positions
- Severity level: High
- Mitigation: Real-time servers are on uninterruptible power supplies and operational facility #1 has a diesel generator, so code can be run manually if machine power is temporarily lost.

Risk Factor #5

- Failure type: Long-term power outage
- Impact: Inability to place orders or modify positions
- Severity level: High
- Mitigation: Server at operational facility #1 can be used to generate orders.

Risk Factor #6

- Failure type: Hardware failure of research servers
- Impact: Loss of research/development data
- Severity level: Medium
- Mitigation: RAID 5/6 used to preserve data integrity, uninterruptible power supplies used to ensure machine uptime, offline backups periodically made (hard drive and/or DVD), offsite backups periodically made to secure, remote server.

Risk Factor #7

- Failure type: Destruction of office (due to natural disaster) or theft
- Impact: Loss of hardware, software, and/or account documentation
- Severity level: High
- Mitigation: Remote server can be used for real-time signal generation, software copies are stored remotely at a commercial repository, documents are kept in locked cabinets, electronic copies of documents are kept on a secure, remote server.