



LIM Business Continuity Brief

July 14, 2008

LIM maintains a systematic approach to business continuity with a disaster recovery plan that accounts for a broad range of possible scenarios. It is the security policy of LIM not to disclose the names or locations of any vendors, off-site facilities or geographic locations of secondary storage systems for the protection of our customers, employees and shareholders interests. Disclosure of individual system details is also restricted so as not to expose any possibility of vulnerability including applications types, versions, and implementation configurations. Administrative capabilities are fully replicated between our Chicago, Illinois main corporate headquarters and our Austin, Texas facility. All technical operations are managed from our Austin, Texas computer facility with a secondary 'HotSite' operating a data warehouse and distribution system.

Sales and support functions are geographically distributed to include our offices in Austin, Chicago, Houston, New York, London and Sydney. Based on the geographic distribution of administration and support staff, business continuity for those functions retains necessary redundancy to mitigate short and long term risk of loss of general corporate operations.

Primary backups of all data and systems are maintained with a scheduled tape rotation and then stored with a bonded agent at an off-site facility. The off-site facility retains all media in a state of the art, climate controlled, secure environment beyond a required minimum radius, yet still within a restricted travel distance from the LIM primary technical location. A Service Level Agreement with the agent outlines mandatory response times for delivery of the media to the Austin facility. There is an alternate plan for media pick-up by company officers should the primary Austin facility become unavailable.

The secondary 'Hot Site' is also located beyond a minimum radius from the primary Austin technical facility. A complete 'core' operating warehouse fully capable of sustaining daily operations for data warehousing, distribution, and support is maintained as a mirror of the primary system. Up to the second replication over a fiber optic native LAN circuit ensures the highest level of integrity for an absolute zero data loss requirement. The mirrored system is periodically switched to primary distribution operations in controlled tests to ensure a seamless activation. The mirrored system also undergoes a scheduled full tape backup restoration and re-synchronization with the primary system to ensure the next order disaster recovery process is in place. Standby office facilities at the hot site include employee cubicles, conference rooms, and kitchen privileges. All individual desktop PC's are also mirrored to a centralized disk based system, also replicated to tape to ensure quick redeployment.

Officers of the company located outside of the Austin area are responsible for security should the local Austin employees become unavailable. Contents of backup tapes are detailed in hard copy documentation in the event that primary systems administrators with common knowledge of these systems are unavailable for the recovery of systems. All recovery documentation includes: equipment lists, software lists and diagrams that are stored electronically on tape in an effort to provide a consolidated recovery package.

LIM operation systems for all data processing, distribution, and operation are fully redundant with all necessary recovery capabilities contained within the Austin, Texas technical facility. HVAC includes a completely independent and fully redundant system capable of sustaining 100% of computer room operations in the event of an HVAC system failure. Additional supplemental HVAC equipment is supplied by normal building operations with management control systems operated by LIM employees. All computer room equipment is powered by distributed UPS systems for protection and isolation from the building power supply. A backup diesel generator system is linked into the UPS power grid and managed by a computerized control system for instantaneous, automated startup during black-out power failures and various brown-out situations. A rigid maintenance schedule including manual startup procedures is practiced weekly.

All system critical hardware has a complete on-site redundancy solution appropriate for the application. The solutions vary from hot standby spares with live replication to cold hardware. Primary policy requires that critical systems follow an internal minimum standards specification using standard enterprise class architecture and Raid disk specifications.

Communication systems are fully redundant including diverse paths, router hardware and remote management security access. Network architecture contains physically and logically isolated subnet structures to create a protected environment for the company's internet, corporate networks, and vendor supplied equipment located in the fire-walled network zone.