

Webcom Data Center

Disaster Recovery Plan

Overview

Webcom's Data Center has developed an environment that relies on automated systems to support its mission and operation. An enterprise wide network of voice and data components ties end users to centralized data sources, telephony resources, a common switching fabric, and external information resources.

Recognizing the high degree to which Webcom and its customers depend on these services, and the criticality of these systems to ongoing operations, dictates that a rational plan be developed which insures the most critical components of these systems can be returned to service in a reasonable amount of time following service interruption.

Assumptions

The plan contains general assumptions, but does not attempt to consider all the possible situations that could occur. Decisions for situations not covered in this plan will be made, as needed, by Webcom's Data Center Management.

The senior Data Center IT staff member on site at the time of the incident will assume immediate responsibility for invoking and implementing this plan. If the situation permits, attention will be given to securing data, and undertaking any and all administrative actions to insure data integrity, and to preserve IT resources.

At the time of occurrence, the senior staff person present, or the first person onsite following an incident will contact the Manger of Information Technology, and senior company management with regard to the need to declare an incident.

Once an incident has been declared this plan will remain in effect until the incident has been substantially resolved.

Invocation of this plan implies that recovery operations have begun, and will continue with the highest priority until essential systems have been restored to service.

Incidents Requiring Action

This plan will be invoked under one of the following conditions:

An occurrence beyond the scope of daily operations has impaired the use of computers, telephony, or data communication facilities in a manner that will have a significant adverse impact on the normal operation of Webcom's services.

An incident has disabled, or is expected to disable the central computing facilities and/or the communications network to the degree that normal operations will be significantly impacted for a period of 24 hours or more.

www.webcominc.com

CONFIDENTIAL

Contingencies

A number of general situations exist which can destroy or otherwise impair computer, telephony, and data network services. This plan considers and plans for contingencies under the following major categories:

- Fire
- Water
- Weather and other natural phenomenon
- Sabotage or breaches of network security
- Environmental interruptions (e.g., excessive temperature and humidity)
- Electrical interruptions

Different levels of severity will necessitate different strategies and types of recovery. This plan covers strategies for:

- Partial recovery - Operating from an alternate site.
- Full recovery - Operating at the current site, possibly with a degraded level of service.

Recovery Team

The Incident Recovery Team will be assembled in the event of a declared incident. The recovery team will be assembled through the use of the Emergency Call list.

The Incident Recovery Team will be comprised of the following:

- Incident Recovery Coordinator - Manager of Information Technology
- Manager of Telephony Services
- Manager of Technical Services
- Help Desk personnel

Additionally, each representative on the Incident Recovery Team will utilize staff with the required technical skill specialties necessary to support recovery activities as required by the expertise required by the particular incident.

In the event of a declared incident the recovery team will convene in the Team Room of Webcom's Data Center. If the declared incident is of such a magnitude that the Team Room is unusable, the recovery team will meet in the parking lot of 10437 Innovation Drive and will utilize their cell phones to coordinate activities.

The responsibilities of the recovery team will be as follows:

Incident Recovery Coordinator The Manager of Information Technology will serve as the Incident Recovery Coordinator. The major responsibilities of this position include:

1. Determine the extent and seriousness of the incident, notifying and updating the Webcom management team of the status of recovery actions.
2. Invoking this plan when an incident occurs.
3. Coordinating priorities for client systems recovery will move ahead with full recovery actions.
4. Supervising recovery activities.

www.webcominc.com

CONFIDENTIAL

Manager of Telephony Services The Manager of Telephony services will assist the Incident Recovery Coordinator to implement recovery actions and will be responsible for:

1. Evaluate and provide recommendations for telephony, and communications systems repair or replacement.
2. Will supervise and coordinate telephony related hardware and software repair and replacement activities with the appropriate vendors.
3. Coordinate system recovery activities with telephony service providers (Time Warner and TDS MetroCom).
4. Keep the Incident Recovery Coordinator and other members of the Management team informed of the status of recovery procedures being implemented.

Manager of Technical Services The Manager of Technical services will assist the Incident Recovery Coordinator implement recovery actions and will be responsible for:

1. Providing a pool of LAN/WAN technicians as required to implement recovery activities.
2. Communicating and coordinating hardware and software replacement with vendors.
3. Keeping the Incident Recovery Coordinator and other members of the Management Team of the status of replacement hardware and software.

Help Desk Personnel Members of the Help Desk staff will assist the Incident Recovery Coordinator implement recovery actions and will be responsible for:

1. Provide liaison between the incident recovery team and Webcom clients.
2. Facilitate and coordinate communications between the incident recovery team and the management and staff of Webcom.
3. Keep the Incident Recovery Manager and other team members informed of the status of recovery procedures being implemented.

Incident Preparation

The ability to respond to an incident, and to fully recover after an incident, requires that this plan and all supporting actions be undertaken on an ongoing basis. Among the general procedures that must be reviewed and updated periodically are:

1. Maintain and update the incident recovery plan.
2. Insure that the Incident Recovery Team personnel are aware of their responsibilities in the event of an incident.
3. Monitor backup procedures to insure that all systems are being backed up, and that the backups are sufficient to restore data in the event of an incident.
4. Maintain and periodically update materials that will be used to recover after an incident. Specifically, network documentation and systems information need to be maintained and stored off site in addition to being posted to the Intranet.
5. Insure that emergency power backup systems are functioning properly and are being tested on a regular basis.
6. Insure that fire detection and fire suppression systems are being tested regularly and are functioning properly.
7. Insure that software distribution media necessary to support system recovery are available.
8. Insure that the Webcom user community is aware of the concept of disaster recovery, our procedures, and how an incident could affect normal operations.

www.webcominc.com

CONFIDENTIAL

Software Safeguards

Tape Backups The backup schedule used to perform tape backups of servers is found attached as Appendix B to this plan. Backup guidelines are for complete tape backups to be performed on the servers nightly Monday through Friday. The backup jobs are scheduled to begin at 10pm nightly. The tape backups are performed using Veritas Backup Exec software. Additionally, each server performing tape backup functions has an associated set of recovery disks that have been created using Veritas' Intelligent Disaster Recovery agent.

Device Configurations Copies of router, firewall and switch configurations are maintained as part of Webcom Data Center's standard network administration procedures. These configurations are included as part of the nightly backup process. Additionally, these system critical files are maintained on a CD ROM and stored offsite as a component of the materials that will be used by the incident recovery team.

Software Media Storage Operating system, service pack, and application media are stored in a fireproof media safe to facilitate rapid recovery actions.

Recovery Procedures

The servers and network infrastructure is covered against loss through insurance. Additionally key networking infrastructure hardware is covered with service agreements to guarantee rapid repair and return to service.

Failure at the Data Center location: When an incident occurs that will cause Webcom's Data Center to use an alternative site, or is such that operations can be restored at the data center site the following steps will be taken:

1. Determine the extent of damage to systems or services, and evaluate if additional equipment and supplies are needed.
2. The Incident Recovery Coordinator will develop a prioritized list of systems to be restored in the event of the failure of multiple critical systems. In the event of the loss of multiple critical systems the highest priority will be placed on the restoration of Internet access and customer web sites. This will be followed by the restoration of telephony, essential processes including accounting, CRM, file and print services, and finally completed services to the user desktop.
3. Obtain approval for the purchases of any needed equipment and supplies.
4. Notify vendors if there is a need for immediate delivery of hardware to bring systems to an operational level.
5. If necessary, notify vendor support personnel that assistance may be required, and obtain their involvement at the earliest opportunity in the restoration process.
6. Review the need for equipment and parts such as electrical cables, patch cables, patch panels and expedite these supplies from Advance Cabling, Graybar, and other vendors as appropriate.
7. Inventory essential equipment and determine what materials can be salvaged and what will need to be ordered.
8. If an alternative location is necessary, the Incident Recovery Coordinator will coordinate the movement of support personnel and equipment to the alternative site.

9. As soon as the necessary equipment has been assembled, load the operating system, load the most current backups, and begin acceptance testing.
10. Determine the priorities for client operations and load any applications required in the order of most critical need.
11. Prepare backups and return the back up materials to sage storage.
12. Commence critical operations resuming production and backup procedures as full data center capacities and operations return to normal status.
13. Establish a schedule to insure all critical support services are made operational.
14. Keep administration, customers, and users informed of status, progress and problems.
15. Coordinate long range plans for a full restoration of services.

Power related failures: The data center is equipped with an APC Silcon 20KV UPS which provides power to all the devices in the data center. In the event of a power failure, the Silcon UPS can provide sufficient power to continue operations. Should a power failure occur, power to the Silcon UPS will be provided by a natural gas generator.

Environmental control systems failures: The data center operates with redundant 3 ton air conditioners. The data center can continue operations in the event one unit fails. The air conditioners are monitored directly by the HVAC management system and service representatives are paged in the event of a failure.

Air temperature, humidity, and power status are also monitored utilizing the out of band monitoring provided with the Silicon UPS. If temperature or humidity threshold are exceeded, or if the UPS detects a power failure pager notifications are sent to the on call staff.

Physical Safeguards

The Webcom Data Center is located at 10400 Innovation Drive, Wauwatosa and is locked 24 hours a day. Access to the data center is limited to IT staff, and select Technical Services staff who assist in supporting the network. Access is monitored by the security system and each access or attempted access to the data center is logged as to the use, date, time, and point of access.

The building within which the data center is located is locked between 6pm and 7am Monday through Friday.

Network Security Issues

Network related problems that are due to a security breach, indications of attempts to circumvent network security, or attempts to attach to secure network services and devices are among the most difficult problems to develop a response plan.

In the event of a suspected network intrusion the following steps will be taken:

1. The individual noticing the unusual activity or suspicious problem will immediately contact the IT Manager, and in his absence the help desk to report the problem and share their observations.
2. A determination will be made on the nature of the problem:
 - o Is the problem a result of a software problem?
 - o Has virus scanning software detected anything unusual?
 - o Is there any indication that files or systems have been tampered with or otherwise damaged?
 - o Is there an indication that there is an attack in progress?
3. If an attack appears to be in progress copies of the firewall logs will be preserved and used to trace the origin of the attack.
4. If a system appears to have been compromised the system will be taken off line and the following actions taken:
 - o The nature of the intrusion will be determined.
 - o If network security has been compromised all administrator, administrator equivalent, service account and remote access passwords will be changed.
 - o All files modified as a result of the intrusion will be removed and replaced with files from last backup previous to the intrusion.
5. Following the recovery actions the Incident Recovery Coordinator will return the affected systems online.

End User Computing Recovery Plan

The security and availability of restorable backups for end user computers are difficult tasks to accomplish and are the responsibility of an individual user.

It is the policy of the Webcom Data Center that all user data be stored on network servers and be filed by customer, project, or functional area. This information is backed up nightly as part of the daily tape backup procedure. Thus, in the event of end user computer failure the user's data files are retained.