Disaster Recovery Plan

Doorway

SOC 2 Criteria: CC5.3, CC7.5

Keywords: Tabletop testing, Disaster Recovery Simulation

Purpose

This policy establishes procedures to recover Doorway following a disruption resulting from a disaster. This Disaster Recovery Policy is maintained by the Doorway Security Officer and Privacy Officer.

Background

The following objectives have been established for this plan:

1. Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
    1. **Notification/Activation phase** to detect and assess damage and to activate the plan.
    2. **Recovery phase** to restore temporary operations and recover damage done to the original system.
    3. **Reconstitution phase** to restore system processing capabilities to normal operations.
2. Identify the activities, resources, and procedures needed to carry out Doorway processing requirements during prolonged interruptions to normal operations.
3. Identify and define the impact of interruptions to Doorway systems.
4. Assign responsibilities to designated personnel and provide guidance for recovering Doorway systems during prolonged periods of interruption to normal operations.
5. Ensure coordination with other Doorway staff who will participate in the Disaster Recovery Planning strategies.
6. Ensure coordination with external points of contact and vendors who will participate in the Disaster Recovery Planning strategies.

Policy

Examples of the types of disasters that would initiate this plan are natural disaster, political disturbances, human-made disaster, external human threats, internal malicious activities.

Doorway defines two categories of systems from a disaster recovery perspective:

1. **Critical Systems**.

These systems host application servers and database servers or are required for functioning of systems that host application servers and database servers. These systems, if unavailable, affect the integrity of data and must be restored, or have a process begun to restore them, immediately upon becoming unavailable.

1. **Non-critical Systems**.

These are all systems not considered critical by the definition above. These systems, while they may affect the performance and overall security of critical systems, do not prevent Critical systems from functioning and being accessed appropriately. These systems are restored at a lower priority than critical systems.

Threat and Risk Assessment and Management

There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

The Doorway IT Risk Assessment documents a full detailed assessment of threats.

Testing and Maintenance

The Security Officer shall establish criteria for validation/testing of a Disaster Recovery Plan, an annual test schedule, and ensure implementation of the test. This process will also serve as training for personnel involved in the plan's execution. At a minimum, the Disaster Recovery Plan shall be tested annually. The types of validation/testing exercises include tabletop and technical testing.

Tabletop Testing

The primary objective of the tabletop test is to ensure designated personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the Disaster Recovery Plan, in a timely manner. The exercises include, but are not limited to:

- Testing to validate the ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis.

Technical Testing

The primary objective of the technical test is to ensure the communication processes and data storage and recovery processes can function at an alternate site to perform the functions and capabilities of the system within the designated requirements. Technical testing shall include, but is not limited to:

- Process from backup system at the alternate site
- Restore system using backups
- Switch compute and storage resources to alternate processing site.

Disaster Recovery Procedures

Notification and Activation Phase

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to Doorway. Based on the assessment of the Event, sometimes according to the Doorway Incident Response Policy, the Disaster Recovery Plan may be activated by the Security Officer and/or CTO.

The notification sequence is listed below:

- The first responder is to notify the CTO. All known information must be relayed to the CTO.
- The CTO is to contact the rest of the team and inform them of the event. The CTO is to begin assessment procedures.
- The CTO is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the CTO is to follow the steps below.

Damage Assessment Procedures:

- The CTO is to logically assess damage, gain insight into whether the infrastructure is salvageable, and begin to formulate a plan for recovery.

Alternate Assessment Procedures:

- Upon notification, the CTO is to follow the procedures for damage assessment with combined DevOps and Web Services Teams.
- The Doorway Disaster Recovery Plan is to be activated if one or more of the following criteria are met:
    - Doorway systems will be unavailable for more than 48 hours.
    - Hosting facility is damaged and will be unavailable for more than 24 hours.
    - Other criteria, as appropriate and as defined by Doorway.

- If the plan is to be activated, the CTO is to notify and inform team members of the details of the event and if relocation is required.
- Upon notification from the CTO, group leaders and managers are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.
- The CTO is to notify the hosting facility partners that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.
- The CTO is to notify remaining personnel and executive leadership on the general status of the incident.
- Notification can be delivered via message, email, or phone.

Recovery Phase

This section provides procedures for recovering the application at an alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.

The following procedures are for recovering the Doorway infrastructure at the alternate site. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal: The goal is to rebuild Doorway infrastructure to a production state.

The tasks outlined below are not sequential and some can be run in parallel.

1. Contact Partners and Customers affected.
2. Assess damage to the environment.
3. Begin replication of new environment using automated and tested scripts. At this point it is determined whether to recover in Rackspace, AWS, GCP, Heroku, Azure, or another cloud environment.
4. Test new environment using pre-written tests.
5. Test logging, security, and alerting functionality.
6. Assure systems are appropriately patched and up to date.
7. Deploy environment to production.
8. Update DNS to new environment.

Reconstitution Phase

This section discusses activities necessary for restoring Doorway operations at the original or new site. The goal is to restore full operations within 24 hours of a disaster or outage. When the hosted data center at the original or new site has been restored, Doorway operations at the alternate site may be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

Original or New Site Restoration

- Begin replication of new environment using automated and tested scripts - DevOps
- Test new environment using pre-written tests. - Web Services
- Test logging, security, and alerting functionality. - Dev Ops

- Deploy environment to production - Web Services
- Assure systems are appropriately patched and up to date. - Dev Ops
- Update DNS to new environment. - Dev Ops

Plan Deactivation

If the Doorway environment is moved back to the original site from the alternative site, all hardware used at the alternate site should be handled and disposed of according to Doorway policy.

Revision History

Version	Date	Editor	Description of Changes
1.0	24.02.2022	Henry Sinclair	Initial Creation