Business Continuity and Disaster Recovery Plan

Table of Contents

Revision History

Name	Title	Comment	Date
[REDACTED]	Program Manager, Security Compliance	Information consolidated into this Plan	25 Mar 2024
[REDACTED]	Program Manager, Security Compliance	Annual Review. Updated logo and doc name	06 Sep 2024
[REDACTED]	Program Manager, Security Compliance	Added BIA and updated links	10 Sep 2024
[REDACTED]	Program Manager, Security Compliance	Linked to IRP. Added lessons learnt from tests and security events or incidents should be incorporated into BC/DR procedures.	11 Sep 2024
[REDACTED]	Program Manager, Security Compliance	Added RTO/RPO for each product in the table.	29 Oct 2024
[REDACTED]	Program Manager, Security Compliance	Added Intel exception for 3 day retention on RDS	15 Nov 2024
[REDACTED]	Program Manager, Security Compliance	Removed documented exception for Intel as they made the change to 7 days retention period. Updated key names with responsibilities. Removed the scope restriction.	08 Jan 2025

Purpose

This document establishes a comprehensive plan to recover Cofense services quickly and effectively following a disruption.

During the notification and activation phase, appropriate personnel are apprised of current conditions and damage assessment begins.

During the recovery phase, appropriate personnel take a course of action to restore the components that experienced the disruption.

In the final, verification phase, actions are taken to verify system processing capabilities to normal operations and deactivate the plan.

Roles and Responsibilities

Business Continuity and Disaster Recovery Owner

The BC/DR (Application) Owner is a member of Engineering management and owns the responsibility for all facets of business continuity and disaster recovery execution for their Cofense service.

The BC/DR Owner performs the following duties:

- Makes the decision on whether or not to activate the BC/DR
- Provides the initial notification to activate the BC/DR
- Notifies and advises the BC/DR team members as necessary
- Designates the BC/DR Coordinator or assumes the role
- Ensures their procedures incorporate lessons learnt from previous tests, security events or incidents

BC/DR Coordinator

The BC/DR Coordinator performs the following duties:

- Leads the response effort once the plan has been activated
- Prioritizes recovery of components
- Facilitates periodic BCP/DR testing exercises
- Manages and monitors the overall recovery process
- Receives updates and status reports from team members
- Sends out communications during recovery
- Issues a recovery declaration statement after the system has returned to normal operations
- Designates key personnel

Engineering Team(s)

The Engineering team performs the following duties:

- Assesses the extent of damage to the information system components
- Estimates the time to recover operations
- Reports updates, status, and recommendations to the coordinator
- Communicates with software vendors as needed
- Restores systems from most current backups
- Maintains current system software configuration information
- Develops recovery effort documentation
- Adds lessons learned into procedures

Security Team

The Security Team performs the following duties:

- Coordinates with the BC/DR Coordinator
- Provides security measures to support the recovery effort
- Provides assistance in investigating the damage
- Ensures that alternate site has access and other security controls if applicable

Business Continuity and Disaster Recovery PHASES

1. Activation and Notification

Activation of the BCP/DR occurs after a disruption, outage, or disaster that may reasonably extend beyond the RTO established for a system. The outage event may result in severe damage to the IaaS provider that houses the system, severe damage or loss of equipment, or other damage that typically results in long-term loss. Once the BCP/DR is activated, the information system stakeholders are notified of a possible long-term outage, and a thorough outage assessment is performed for the information system. Information from the outage assessment is analyzed and may be used to modify recovery procedures specific to the cause of the outage.

2. Recovery

The Recovery phase details the activities and procedures for recovery of the affected system. Activities and procedures are written at a level such that an appropriately skilled technician can recover the system without intimate system knowledge. This phase includes notification and awareness escalation for communication of recovery status to system stakeholders.

Recovery Time Objective (RTO)

- RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources and supported mission/business processes.
- This is defined by each SaaS Cofense product or corporate service.

Recovery Point Objective (RPO)

- The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage.
- This is defined by each SaaS Cofense product or corporate service.

3. Verification

The Verification phase defines the actions taken to test and validate system capability and functionality at the original or new location. This phase consists of these major activities: validating data and operational functionality followed by deactivation of the plan.

Validation procedures include functionality or regression testing, concurrent processing, and/or data validation. The system is declared recovered and operational upon successful completion of validation testing.

Deactivation includes activities to notify users of system operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future events.

Data Backup Readiness and Restore Testing

Based on system, capacity and availability issues, databases are subject to full data backups or may employ database replication technology as a means of providing the assurance that databases can be rapidly recovered in the event of a disaster.

Backups	Minimum Requirement	Maximum Requirement
Frequency	Daily	n/a
Retention Period	7 Days	30 Days
Restore Testing	Annually	n/a

Business Impact Analysis (BIA)

The purpose of the BIA is to document recovery priority (criticality) by identifying service disruption outcomes and the business impact from a customer security perspective.

SaaS Application	Application Owner	Service Disruption	Business Impact	Recovery Priority (Criticality)	RTO (hrs)	RPO (hrs)
Triage	[REDACTED]	If Triage is unavailable, customer SOC teams can't efficiently analyze reported phishing emails.	High	1	3	24
Reporter	[REDACTED]	If Reporter is unavailable, customers can't automatically report real phishing threats to their security team.	High	1	6	24
Vision	[REDACTED]	If Vision is unavailable, customers can't easily quarantine/pull the malicious emails.	High	1	24	24
PhishMe	[REDACTED]	If PhishMe is unavailable, customers can't effectively send phishing simulations to their personnel or gather statistics for training and re-training purposes.	Moderate	2	24	24
Intelligence	[REDACTED]	If Intelligence is unavailable, customers will be less aware of attacks happening to other organizations globally.	Moderate	2	48	24

LMS	[REDACTED]	If LMS is unavailable, customers will not easily be able to train and re-train staff for security awareness purposes.	**Low**	**3**	**24**	**24**

BC/DR Procedures and Annual Testing

The business continuity/disaster recovery procedures for SaaS SOC 2 products shall be tested annually. The procedures shall incorporate lessons learned from previous tests, security events or incidents in sync with Cofense SaaS - Incident Response Policy and Procedure. [LINKS HAVE BEEN REDACTED]

Triage Hosted and MSSP - Business Impact Analysis and Disaster Recovery Procedure

Reporter SaaS - Business Impact Analysis and Disaster Recovery Procedure

Vision - Business Impact Analysis and Disaster Recovery Procedure

PhishMe - Business Impact Analysis and Disaster Recovery Procedure

Intelligence - Business Impact Analysis and Disaster Recovery Procedure

LMS - Business Impact Analysis and Disaster Recovery Procedure