By Lillian McGowan

Executive Summary

In October, a major Amazon Web Services (AWS) cloud service disruption impacted a wide range of organizations that depend on AWS for critical operations. While AWS ultimately restored services, the duration and scale of the outage revealed limitations in incident response speed, communication clarity, and customer accessibility during large-scale cloud failures.

This document presents an improved incident response plan based on analysis of that event. Rather than simply documenting what occurred, this plan focuses on what could have been done faster, clearer, and more effectively to reduce operational impact for customers and improve overall response coordination.

The goal of this plan is to demonstrate how a large cloud-dependent organization could implement a more resilient, customer-centric, and time-efficient incident response strategy during widespread cloud outages.

By Lillian McGowan

Incident Context

- Incident Type: Large-scale cloud service disruption
- Provider: Amazon Web Services (AWS)
- Timeframe: October (publicly reported event)
- Customer Impact:
    - Service downtime
    - Loss of access to dependent systems
    - Operational delays across multiple industries

Many affected organizations relied heavily on AWS, which limited their ability to pivot quickly when services degraded.

Key Challenges Observed

The following issues were widely experienced by customers:

1. Extended Recovery Time

   Services took a significant amount of time to fully stabilize, extending business disruption.

2. Limited Customer Access to Alternatives

   Many organizations were heavily concentrated on AWS, leaving few immediate failover options.

3. Delayed or Vague Communication

   Customers struggled to understand:

    - What was impacted
    - What actions they should take
    - How long disruptions might last
4. Operational Bottlenecks

   Internal teams were often waiting on provider updates instead of executing predefined mitigation steps.

By Lillian McGowan

Where Traditional Incident Response Fell Short

While standard incident response steps were followed, the scale of the outage exposed weaknesses:

- Incident response plans assumed partial failures, not ecosystem-wide disruption
- Communication models did not scale well to millions of customers
- Many customers had no pre-approved decision authority to act independently
- Response actions were reactive rather than pre-positioned

This plan addresses those gaps.

Improved Incident Response Objectives

The optimized response model focuses on five priorities:

1. Speed over perfection
2. Customer autonomy during outages
3. Clear, repeated, plain-language communication
4. Pre-approved technical actions
5. Parallel recovery, not sequential recovery

Enhanced Incident Detection & Escalation

What Should Have Happened Faster

Improvement Actions:

- Correlate alerts across regions immediately
- Auto-escalate to executive incident command within minutes
- Declare a “Major Cloud Dependency Incident” earlier

Optimized Detection Flow

- Automated monitoring detects regional anomalies
- Correlation engine confirms multi-service impact
- Incident severity automatically escalates to Critical
- Full incident response team activated immediately

This reduces hesitation and decision delays.

By Lillian McGowan

Improved Response Structure

Problem Identified

Teams waited for confirmation or approvals before acting.

Optimized Solution

- Pre-authorize response actions during cloud dependency failures
- Empower incident commanders to:
  - Pause nonessential workloads
  - Activate failover plans
  - Communicate independently of provider updates

Better Communication Strategy (Major Improvement Area)

What Went Wrong

Customers lacked clarity and actionable guidance.

Optimized Communication Model

Every update must answer three questions:

1. What is impacted?
2. What should customers do right now?
3. When is the next update?

Communication Improvements

- Plain-language summaries (no technical jargon)
- Fixed update cadence (every 30–60 minutes)
- Separate technical and non-technical updates
- Clear acknowledgment of customer frustration

This builds trust even during prolonged outages.

By Lillian McGowan

Faster Containment & Mitigation Strategy

Key Improvement: Parallel Response

Instead of waiting for full service restoration:

- Shift eligible workloads to secondary regions
- Temporarily disable non-critical services
- Reduce dependency load on failing services
- Activate manual business processes where needed

Why This Matters

Even partial recovery reduces customer impact dramatically.

Recovery Optimization

What Should Have Been Done Better

- Gradual restoration with load controls
- Priority restoration for critical customers
- Verification checkpoints before declaring stability

Optimized Recovery Flow

1. Restore identity and access services
2. Validate monitoring and logging
3. Bring core workloads online
4. Restore secondary services
5. Confirm customer access

By Lillian McGowan

Post-Incident Review: Turning Pain Into Progress

What This Event Taught Us

- Cloud concentration risk is real
- Customers need more autonomy during outages
- Communication speed matters as much as technical recovery
- Incident response plans must scale beyond “normal” failures

Strategic Recommendations

Key Improvements Going Forward

- Multi-cloud or hybrid contingency planning
- Regular large-scale outage simulations
- Customer-facing incident guidance playbooks
- Faster internal escalation triggers
- Stronger business continuity alignment

These steps reduce downtime, customer frustration, and long-term risk.