Fine Tuning Incident Response

Digital Directions 2022

1

Evolution of Incident Management

The Katrina wake-up Call

- *Disaster Recovery* was the norm. System Recovery Time Objectives were commonly 48 hours or more so expectations were fairly low
- Plans had never been tested to that degree.
- Technology was always in focus, but the *people* side of the event was often not
- Most banks experienced at least some empathy

Higher Expectations in 2022

- Disaster *Resilience* is the new normal.
- Business moves at a faster speed.
- There is less empathy and an expectation that service will not be interrupted.
- CoVid proved effectiveness of remote work
- Plans reflect more of a practical, functional, and human resource focused approach

2

Lessons Learned

Be strategic in your planning

- Implement an incident response plan based on a solid framework
- There will be unexpected fires, but good planning will buy you the time to put them out
- Be creative

Communicate

- Have a solid plan for internal and external communications
- Consider an emergency notification service
- Consider an incident response application

Strive for technology resiliency

- Replicate rather than back up
- Automate recovery where possible

Take care of your people

- Resilient technology may not help if there is no one there to use it
- Set expectations and understand constraints

Create partnerships

- Retain vendors for critical services
- Familiarize yourself with local government emergency operations
- Encourage partnerships within and outside of the company

3

Strategic Planning

Incident Command System (ICS) modified to fit our Plan

- ICS works well for those who work in the field full time
- Terminology should be clear to those who rarely have to use it
- Not necessary to all be in one place, but it helps for big events

Crisis Teams

- Executive Decision Team
  - Executives
  - Who make big decisions
- Core Crisis Team
  - Those who will be involved in any event
  - Think Facilities, Technology, HR, Marketing, etc.
- Regional Crisis teams
  - Regional leaders
  - Critical regional associates
- Business Unit Coordinators
  - Those responsible for line of business planning
  - Also assist in deployments

4

Communicate

Everyone should know their role, even if they don't have one

- Responder designations
- Related Human Resources policy

Set expectations for timing and frequency of communications

- No guarantee technology will be available
- Not everyone will have access to communication channels

Consider an emergency notification service

- Can use for checking in on associate well-being
- Can also poll associates for critical needs or availability for work

Leverage HR, Legal, and marketing

- Can help get the message out
- Can make sure it's the right message

5

Strive for Technology Resilience

Take advantage of rapidly evolving technology

- Manual restoration of backup has moved to automated recovery of replicated data or other resilient technologies
- Reduces impact to company, associates, and clients

Understand what you have and what is critical

- Business Impact Analysis
- What are your most critical, time-sensitive, client impacting applications
- What supports these applications

Test

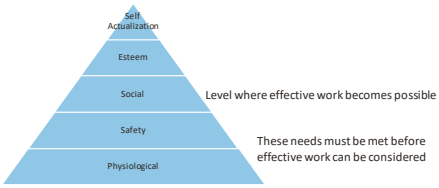
- Builds confidence in processes
- Even a failed test is a good test

6

Take Care of Your People

Maslow's Hierarchy of Needs

- Abraham Maslow proposed this psychology theory in 1943, and it is frequently used in the business world in functions that deal with people.
- Certainly applies to crisis/incident response



7

Take care of Your People

Need to understand the associate's perspective

- What seems trivial to one person may be a priority to another
- Failure to prepare may lead to responder team issues

Associates need to understand personal responsibilities

- Associates should plan ahead for their families
- Does a responder have too much family responsibility?

Consider what they have been through it before?

- Hurricane Katrina, Hurricane Laura, Hurricane Ida
- Trauma response – Anxiety, trouble focusing

Set expectations with policy

- Deployment policy
- Expense reimbursement

Consider assistance post event

- Food
- Fuel
- Hard to get items

Consider your community

8

Partnerships

Mobile Recovery and Equipment on Retainer

- Financial centers onsite in 24 hours. Operational in 48 hours
- Includes generators, IT equipment, bathrooms, satellite, cellular

Fuel Contracts

- Keeps generators filled and helps associates get to work
- Also help with associate personal generators

Remediation

- Stationed outside impacted area
- Ready to move in, assess, and repair facilities as necessary

Housing

- Disaster recovery housing vendor establishes contracts with hotels
- Acquires hotel rooms as need during event

Weather Service

- Pinpoint weather forecasts for critical locations
- Meteorologist available 24/7 available to discuss forecasts

Government Agencies

- Re-entry processes

9

Cyber - The Business Side Response

Key players

- Legal, Compliance, Information Security, Insurance
- Add relevant lines of business as needed (marketing, products, HR)
- Law enforcement

Insurance

- Cyber, ransomware, business interruption
- Insurance company should be informed

Key Partners

- Outside Counsel
  - Attorney client privilege
  - May consider engaging vendors through outside
- Crisis Management Consultants
  - May be promoted by insurance
  - Can take over efforts to allow company to operate BAU
  - Can facilitate testing

10

Questions

11