So You’ve Had a Disaster Now What?

Michael Solomon
June 2016
Agenda

- Where do I even start?
- What's really important?
- What does “recovery” really mean?
- How do I get there?
What is a disaster?
  Unplanned interruption of normal business
This can be a HUGE topic
  We’re just covering the basics today
You’ve heard it all before
  Planning is important
OK, so ...
Results of a live poll of attendees of the talk during PUG Challenge 2016
Now you know why we’re here
Disaster recovery is all about minimizing surprise and confusion.
Cessna 172 cockpit. What do you do if the engine quits right after takeoff?
(Rotate 55 KIAS, climb 70-80 KIAS)

1) Aviate
2) Navigate
3) Communicate
Specific steps for handling engine failure in different flight regimes.
Success depends on the quality of your plan and the readiness of your team.

Medical emergency (someone has to take the lead):
A. Assign someone to call 911/go for help
B. Send someone else for a first aid kit/supplies
C. Assess situation
D. Render aid
Think it through
Before the disaster
What do you really need for operations?
Low tech alternatives may be fine
Write it down

The only way to retain and communicate

What if you aren’t available?
Prioritize

You can’t do everything
Avoid wasting time
- Recovery - The point at which you can carry on
- Restore ≠ Recovery
  - *prorest* isn't enough
  - More than just backups (or even replicated databases)

The point at which you can carry on
Recovery Point Objective (RPO)
How long to get there?
Recovery Time Objective (RTO)
Recovery Point Objective (RPO)
How long to get there?
Recovery Time Objective (RTO)
RPO and RTO defined by business
Not IT
How do we get there?

- **Policy**
  - Support from the top
  - No policy = no support

- **Plan**
  - Plan for the worst
  - BCP vs DRP

- **Prepare**
  - Staff and supplies
  - Awareness and training

- **Perform**
  - Follow the plan

**BCP vs DRP**
- DRP recovers data and infrastructure (short term)
- BCP restores business process (long term)
But *where* do we start?

That’s all great, but how do we develop a plan?
Gamification
RPG
LARP
OK, not that type of RPG!
This is a picture of a real Tabletop Exercise (simulation)
Walkthrough your plan (OR see how hard it is to “make it up as you go” if you don’t have a plan)
Example challenge scenario (segment 1)

- Small fire just outside the data center, setting off the alarm system
- Sprinkler extinguishes the fire by the time the fire department arrives
- The building has been evacuated
- Personnel and the media are aware of what happened
- Then, as people begin to go back inside
  - The receptionist takes a call from someone who indicates that the fire is "only the beginning" because the company hasn't treated him right

What do you do?

Let the audience make suggestions.

Tips:
1) Who does the receptionist call?
2) When does HR get involved?
3) Who answers media questions?
4) Should you call LE? Who calls? Who do you call?
5) Do you let employees back into to building?
## DRP Planning steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Impact Analysis (BIA)</strong></td>
<td>- Identify critical business functions</td>
</tr>
<tr>
<td></td>
<td>- Identify risks</td>
</tr>
<tr>
<td><strong>Prioritize</strong></td>
<td>- Risk value</td>
</tr>
<tr>
<td></td>
<td>- Cost of remediation</td>
</tr>
<tr>
<td><strong>Select Controls</strong></td>
<td>- Preventative / Detective / Corrective / Compensating</td>
</tr>
<tr>
<td></td>
<td>- Use multiple types</td>
</tr>
<tr>
<td><strong>Document</strong></td>
<td>- Clear and succinct</td>
</tr>
<tr>
<td></td>
<td>- General target audience</td>
</tr>
<tr>
<td><strong>Test</strong></td>
<td>- Tabletop exercises</td>
</tr>
<tr>
<td></td>
<td>- Escalating reality tests</td>
</tr>
</tbody>
</table>
Business Impact Analysis - BIA

Identify each critical business functions
- Must have upper management support
- What functions are critical to the business (not IT)?

Consider disruption impact
- Lost/delayed revenue / Increased expenses
- Fines/penalties / Reputation

Timing and duration
- Does disaster timing matter?
- How long can you be down?

Methods
- Questionnaire
- Focus group
- Interview
Risk Assessment

Start with
the BIA
report

Similar info
gathering
techniques
as BIA

Deliverable
– Prioritized
Risk
Register

Main
purpose –
Identify
risks

Main
assessment
techniques
• Qualitative
• Quantitative
Control selection (Risk Management)

Select one or more controls for each risk
  • Consider cost and effectiveness

Control types
  • Preventative
  • Detective
  • Corrective
  • Compensating

Best way to handle disasters: Avoid them!
Plans

Start from the beginning
- What constitutes a disaster?
- Who makes that call?
- Who needs to be contacted?
- What if communications are down?

How do you escalate?

How do you get to your RPO within your RTO?

How can I mess this up?

- Sloppy BIA
- Focus on technology
  - Planning and solutions
- Process too complex
- Lack of
  - Testing
  - Maintenance (configuration drift)
  - Awareness/training
Readiness depends on testing.
As you move down the list, risk increases. Only execute a cutover test if mandated or if you’ve been through the other tests successfully!
Disaster strikes. Time for a real test.
1. Protect people first!
2. Communicate- Ops/Mgmt/HR/PR/Utilities/Vendors/Agencies/LE-
   Know contact info (and specific names)- What if phones/cell service is
   out?
3. Coordinate- Who's responsibility is this?- SLA, etc.- What needs to be
   recovered? (service/hardware/software)
4. 4. Make the call and follow the plan
“It is better to be prepared than surprised”

- Michael Yousef
www.solomonconsulting.com
Resources

- NIST SP 800-34 “Contingency Guide for Information Technology Systems"
- ISO 17799
- COBIT
- DRI International (https://www.dri.org/)
- Michael Solomon (michael@solomonconsulting.com)