Rethinking Risks and Recovery Strategies

Business Continuity Planners Association
April 9, 2015

Roger Peters - Background

• 20+ years of business continuity and risk management consulting experience
• Helped 200+ companies develop or enhance their business continuity and IT recovery plans
• Led a national business continuity and technology risk consulting practice
• Founded Continuity Onward, Inc. to help companies enhance their business continuity and technology governance programs
Time for Spring Cleaning

- Review risk assessments
  - Determine if any new risks should be added
  - Consider new perspectives on business impacts
- Can some “painting” help highlight key issues and exposures to leadership?
- Should any new “green risk” initiatives be identified?

Ongoing Continuity Challenges

- Many moving parts in our organizations
- Limited resources
- Support constraints
- Changing risk profiles
  - Human
  - Technical
  - Environmental
- Unexpected event combinations
- Visits from “Murphy”
Reconsider Single Points of Failure

• Assessment starts small and builds up
  – Systems – components, servers, data centers, etc.
  – Networks – interface cards, routers, channels, etc.
• Do we take the concept far enough in our plans?
  – Infrastructure
  – Facilities
  – Staff
  – Data, etc.

Famous Site in Business Continuity History

April 13, 1992: Great Chicago “Leak”; Chicago River at the Kinzie Street Bridge
Growing Risk of Unexpectedly Severe Weather

Facility Flooding Considerations

- Considerations may apply after external or internal flooding – ex. rain or sprinkler discharge
- Structures may need to be inspected prior to resuming even limited access
- Areas may be off-limits, preventing salvage operations for undamaged data and equipment
- Damage assessments may be lengthy
- Power restoration may be dependent on the entire facility or area being repaired
- Decontamination may be required
- Mold grows quickly and can be hazardous
Facility Flooding Considerations

- Water can follow electrical cables like a wick, causing damage to components above the water levels
- Elevators and escalators may require extensive repair and extended downtime to get parts
- Mitigation and repair resources may be limited during regional disasters
- Review possible facilities impact on staff and ADA compliance
- Determine strategies in advance whenever possible

Increased Fire Risks From Droughts

- Potential fire, smoke and water damages for facilities
- Air quality issues for staff
- Shelter in place or shut down facility decisions
Reconsider Facility Risks

- Quiet suburban location
- Low traffic levels
- New construction
- Good elevation for drainage

Google Street View, Sept. 2013

July, 2014
View from the street

July 2014

A direct hit to the gas meter
Salvage Procedures

- Review resource salvage procedures
- Timely damage assessments and salvage operations can reduce potential losses and reduce the recovery times
- Define damage assessment and salvage teams
  - Consider the facility and staff capabilities for the teams - ex. retrieving disk drives from the 20th floor without working elevators
- Efforts may need to be coordinated with emergency responders, facilities management, engineers/contractors, etc.
  - Initial facility access may be very limited

Sample Damage Assessment Form Extract

<table>
<thead>
<tr>
<th>Damage Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access – Y/N</strong></td>
</tr>
<tr>
<td><strong>Type(s) of damage</strong></td>
</tr>
<tr>
<td><strong>Damage Levels:</strong></td>
</tr>
<tr>
<td>Severe</td>
</tr>
<tr>
<td>Critical</td>
</tr>
<tr>
<td>Minor</td>
</tr>
<tr>
<td>Usable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Damage Levels:</th>
<th>Access</th>
<th>Fire</th>
<th>Smoke</th>
<th>Water</th>
<th>Debris</th>
<th>Other</th>
<th>Severe</th>
<th>Critical</th>
<th>Minor</th>
<th>Usable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work Areas:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HVAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Water Supplies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical Records</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Damage Description</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utilities</td>
<td></td>
</tr>
<tr>
<td>Work Areas</td>
<td></td>
</tr>
<tr>
<td>Computer Systems</td>
<td></td>
</tr>
<tr>
<td>Phone Systems</td>
<td></td>
</tr>
<tr>
<td>Critical Records</td>
<td></td>
</tr>
<tr>
<td>Work in Progress</td>
<td></td>
</tr>
</tbody>
</table>

©2015, Continuity Onward, Inc.
Salvage Operations

• Plan asset/resource triage operations as soon as safety conditions permit

• Asset salvage plans should consider:
  – Security requirements
  – Salvaged asset assessment space
  – Asset tracking processes
  – Repair requirements
  – Transit to/from third-parties for restoration
  – Estimated repair times
  – Redeployment plans
  – Scrapped assets, etc.

Evolving Technical Threats

• Have new systems and applications in your organization brought new technical and security risks to assess and mitigate?
  – Networks
  – Cloud services
  – Cell phones
  – Smart devices
  – Bring Your Own Device (BYOD)
  – Internet of Things (IoT)
  – Big data
Internet Outages

- Many recovery plans are dependent on the Internet without having a secondary plan
- The Internet contains many single points of failure and weaknesses that may be overlooked
- Upgrades to fiber-optic cables increase capacity while concentrating data paths
- Expanded broadband access areas may not get adequate back-up provisions

Northern Arizona Internet Outage

- February 26, 2015: Apparent Vandalism
  - CenturyLink fiber cable buried in the desert was apparently cut by a vandal around noon
  - Outage impacted Flagstaff to northern Phoenix areas, including Prescott and Sedona
  - Disrupted landline phones, computers, ATMs, POS devices and cell phones
  - 911 services were disrupted in some areas
  - Services were not fully restored until 3:00 AM the following day
Cell Phones and Smart Devices

- Networks may become overloaded during significant incidents
  - Increased call volumes plus pictures and video can create severe spikes in network traffic
- Storms may impact cell towers reducing access and capacity
- Cell, land-lines and Internet may share the same channels and be lost simultaneously
- Battery life is limited on many devices
  - Have methods to extend battery life been shared?

Cell Phone and Smart Devices

- Training on contingency procedures can help increase their effectiveness
  - Battery conservation
  - Temporary charging producers
    - Car chargers, charging stations, USB cables, etc.
  - Reminder that text messages are more likely to get through than calls during capacity spikes
- Watch for new opportunities through new devices
Watch for Storms in the “Cloud”

- 2014: Joyent Cloud “dissipated”
- 2/29/2014: Microsoft Azure Cloud leap-year glitch, 1+ day outage
- Google App Engine data center – power caused 25% of servers to fail, back-up servers were overloaded, fail-over to the back-up center failed
- Amazon EC2 – Software bug knocked some servers offline, triggering a “re-mirroring storm” that left some customers down four days
- SalesForce.com – Periodic Oracle upgrade problems extended over 4 months

Source: Continuity Insights; Can You Trust Your Public Cloud?, Bill Highleyman, Managing Editor, Availability Digest
www.continuityinsights.com/blogs/2015/02/can-you-trust-your-public-cloud

Review Cloud Servicing Exposures

- Periodically assess vendor viability
- Check SLAs but they’re almost worthless if they aren’t realistic
- Verify the cloud isn’t a single point of failure
- Review replication and systems failure procedures
- Verify data back-up procedures and locations
- Review SSAE 16 servicer controls and user control requirements
- Review service provider recovery test results for critical applications if possible
- Ensure your procedures include cloud failures
Computer Crime Threats Continue

- 4/7/2015 Survey by the Organization of American States and Trend Micro show increased incidences of attacks designed to destroy data

2015 OAS/Trend Micro Survey

- Other statistics from the 575 security leader respondents
  - 76% indicated that attacks are growing in sophistication
  - 53% saw an increased number of incidents
  - 52% did not have an increase in their cybersecurity budgets in the prior year
  - 54% reported having a disaster recovery plan
Human Threats Continue to Increase

- Expect increased ransomware incidents
- Homegrown terrorism
- Complex systems increase the potential for service disrupting errors
  - Are procedures for critical operations up-to-date?
  - Can any high-risk routines be automated?

3/6/2015: First H5N2 Avian Influenza Outbreak in MN

- Ground-zero for a future jump to humans?
4/7/15: 8th Confirmed H52N MN Case

- The Minnesota Department of Health is working directly with poultry workers at the affected facility to ensure that they are taking the proper precautions.
- As a reminder, the proper handling and cooking of poultry and eggs to an internal temperature of 165 °F kills bacteria and viruses.

Review Internal Procedures

- Degree of business unit plan ownership can lead to inconsistent procedures and recovery capabilities
- Interdependencies with other units can degrade an entire organization’s recovery
- Consider evaluating key criteria across departments, locations and business to identify the “weakest links”
  – Develop plans to enhance consistency
Selected procedures to consider for plan consistency assessments

< --- Time --->

<table>
<thead>
<tr>
<th>Pre-incident Alerts</th>
<th>Incident Occurrence</th>
<th>Incident Response</th>
<th>Recovery Phase</th>
<th>Return to Normal</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Develop plan</td>
<td>• Fast or slow onset</td>
<td>• Verify staff</td>
<td>• Implement recovery plans</td>
<td>• Return to normal schedules and workloads</td>
</tr>
<tr>
<td>• Mitigate risks</td>
<td>• Full impact is uncertain</td>
<td>• Assess damage and impact</td>
<td>• Activate alternate locations</td>
<td>• Return to permanent facilities</td>
</tr>
<tr>
<td>• Train and test</td>
<td>• Coordinate with emergency responders</td>
<td>• Declare the disaster</td>
<td>• Obtain recovery resources</td>
<td>• Inform significant third-parties</td>
</tr>
<tr>
<td>• With advanced warning:</td>
<td></td>
<td>• Active Command Center and alternate sites</td>
<td>• Recover/re-build work in process</td>
<td>• Assess the incident</td>
</tr>
<tr>
<td>- Implement mitigation steps</td>
<td></td>
<td>• Activate recovery plans and teams</td>
<td>• Recover IT systems and data</td>
<td>• File insurance claims</td>
</tr>
<tr>
<td>- Back-up systems</td>
<td></td>
<td>• Salvage assets</td>
<td>• Recover critical processes</td>
<td>• Adjust recovery plans</td>
</tr>
<tr>
<td>- Protect assets</td>
<td></td>
<td>• Requisition recovery resources</td>
<td>• Inform significant third-parties</td>
<td>• Adjust to the “new normal”</td>
</tr>
<tr>
<td>- Dismiss staff</td>
<td></td>
<td>• Inform significant third-parties</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Emergency Communications

• Communications needs can be complex
• Review your communications points
• Traditional and social media communications need to be considered

Graphic source: Ready.gov
Communications Plans

• Determine whether adequate consideration has been given to Legal, Human Resources and Public Relations issues
• Verify that corporate, facility and department plans address internal and external communications needs
  – Individual plans may reference a corporate-wide plan with specific responsibilities for each
  – Ensure all levels understand their responsibilities and limitations

Communications

• Have emergency communications procedures been institutionalized through plan training and exercises?
  – Leadership and staff need to know how to react if normal communications are disrupted
  – Factors that can influence plans, exercises and education requirements include:
    • Interactions with emergency responders
    • Business functions and interdependencies
    • Process criticality and impact on stakeholders
    • Staff locations
    • Staff turnover
    • Recovery complexity
    • Business specific requirements
    • Other considerations
Communication Forms

• Review capabilities to enhance recovery management team views of the recovery
  – Ex. more access to recovery dashboards, staffing, critical process status, etc.
    • Procedures, monitors, projectors, etc.
• Pre-defined forms for post-incident use can facilitate communications, enhance clarity and reduce information losses
• Ensure forms are readily accessible after any type of incident

Selected Incident/Recovery Forms

Staffing Forms:
• Staff Verification Checklist
• Staff Tracking Form
• Hourly Time Reporting Form
• Redirected Telephone Numbers
• Temporary Work Locations
• Staff Assistance Request
• Illness/Absence Tracking Form
• Personal Injury Report

Communications Forms:
• Recovery Status Report
• Communications Log
• Media Message Planning Form
• Media Contact Summary
• Media Communications Form
• Social media monitoring/alerts

Incident Assessment Forms:
• Damage Assessment Team
• Salvage Team
• Bomb Threat Report
• Damage Assessment Report
• Incident Report
• Post-Recovery Incident Assessment Summary
• Incident History

Technology Forms:
• Computer Incident Report
• Salvaged Equipment Form
• Impaired Equipment List
• Equipment Sent For Repair or Scrap
• Technology Sign-Out Form
• Technology Sign-Out Summary
• Help Desk/Trouble Report
Selected Incident/Recovery Forms

- Consider additional forms to meet your requirements
- Look for opportunities to summarize information using dashboards
- Ensure staff are trained on forms use

Financial Forms
- Purchase Order Form
- Purchase Order Log
- New Vendor Form
- Significant Expense Authorizations
- Manual Check Form
- Disaster Related Travel
- Recovery Expense Report

Summary

- Spring is a good time to reconsider risks and mitigation strategies
- Small initiatives could create significant benefits
- Look for ways to enhance management support
- Demonstrate progress and celebrate successes!
Questions??

Thank You!

Roger Peters CBCP, CGEIT
612-360-3603
rpstrmn1@gmail.com
LinkedIn.com/in/RogerPeters1

©2015, Continuity Onward, Inc.