Rethinking Risks and Recovery Strategies

Business Continuity Planners Association

April 9, 2015

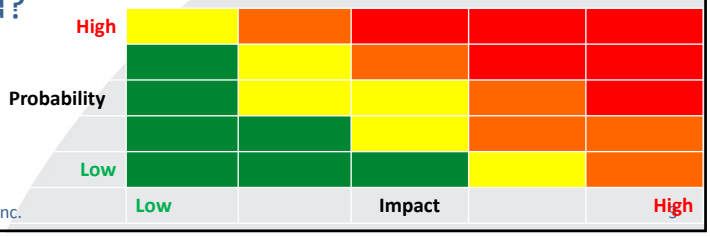
Roger Peters CBCP, CGEIT
612-360-3603
rptrsmn1@gmail.com

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

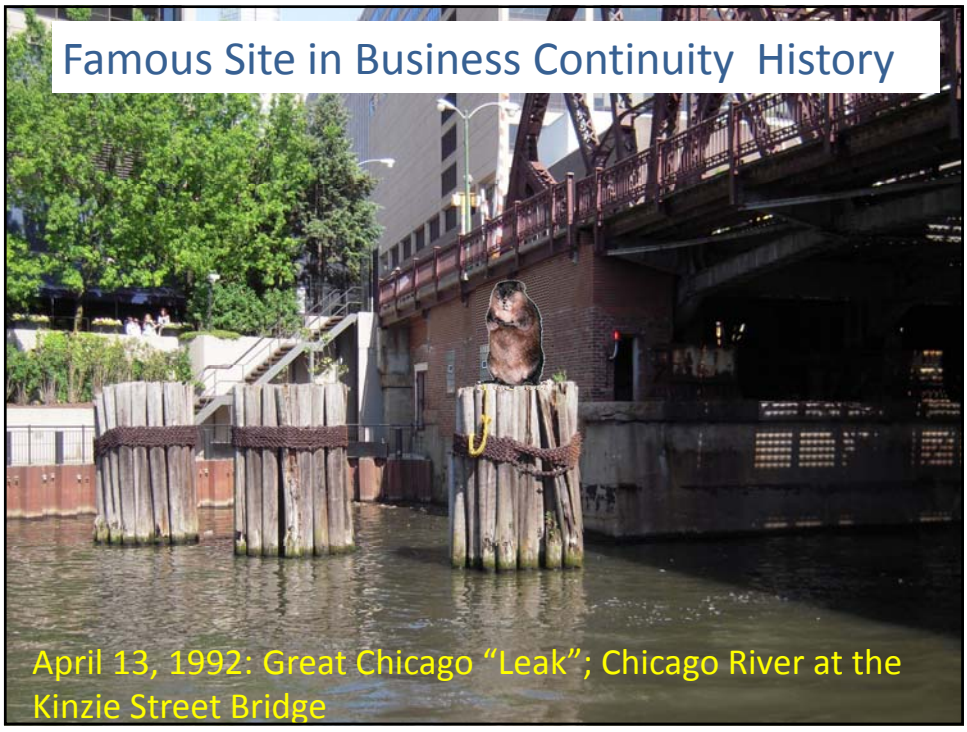
- Many moving parts in our organizations
- Limited resources
- Support constraints
- Changing risk profiles
  - Human
  - Technical
  - Environmental
- Unexpected event combinations
- Visits from "Murphy"

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.

 5

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

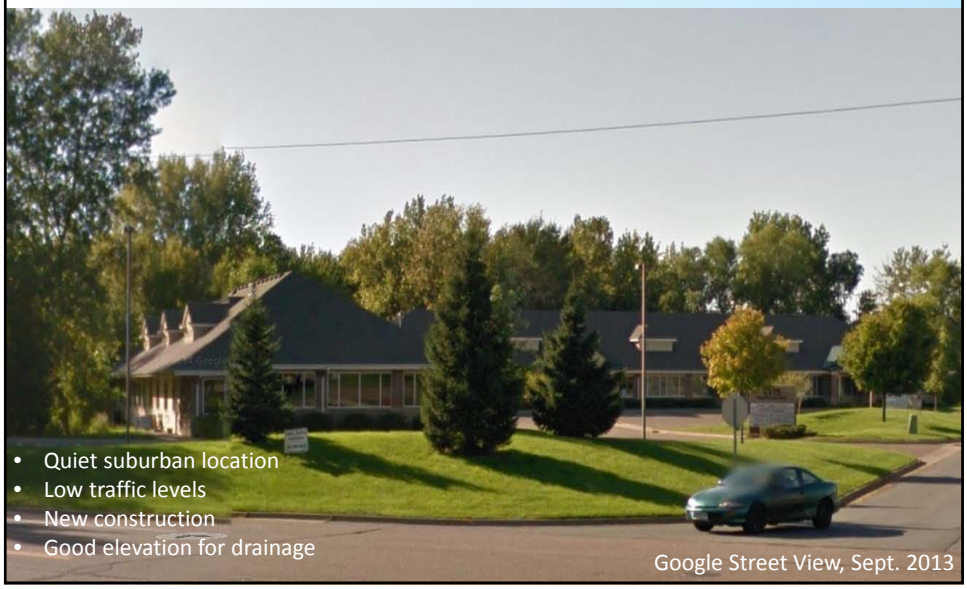
 9

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

10

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

Damage Summary

Access – Y/N	Indicate whether the area to assess is accessible or if safety hazards prevent access.
Type(s) of damage	Indicate all types of damage that exists in the area being evaluated. Explain "Other" damage.
Damage Levels:	Mark an "X" in the estimated damage levels for each of the items being assessed in the table below.
Severe	Extensive damage, lengthy relocation or a move is required, servers must be replaced, and paper records have significant damage and must be quickly conserved to be salvaged.
Critical	Significant damage to the facility but restoration within 30 days is likely, servers appear to be usable but several desktop systems are damaged, critical records have minor damage.
Minor	The facility is likely to be usable within a week, servers are intact, some user computers may require clean-up or replacement, critical records show only minimal damage.
Usable	No relocation required though some clean-up may be necessary, no/minimal damage to user computers is evident, critical records appear to be intact or only minimal damage.

Damage Levels:	**Access**	**Fire**	**Smoke**	**Water**	**Debris**	**Other**	**Severe**	**Critical**	**Minor**	**Usable**
Work Areas										
Electrical Service										
HVAC										
Water Supplies										
Computer Systems										
Phone Systems										
Critical Records										
Work-in Process										
Other:										

Damage Description	**Comments**
Utilities	
Work Areas	
Computer Systems	
Phone Systems	
Critical Records/Work in Process	

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

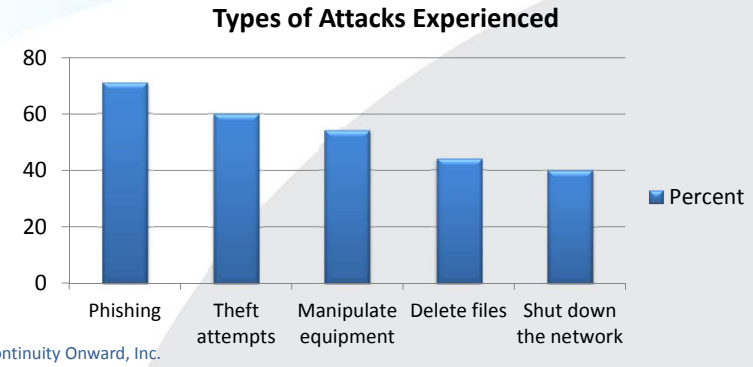
Source: Continuity Insights; Can You Trust Your Public Cloud?, Bill Highleyman, Managing Editor, Availability Digest
www.continuityinsights.com/blogs/2015/02/can-you-trust-your-public-cloud

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 cyber-security budgets in the prior year
  - 54 % reported having a disaster recovery plan

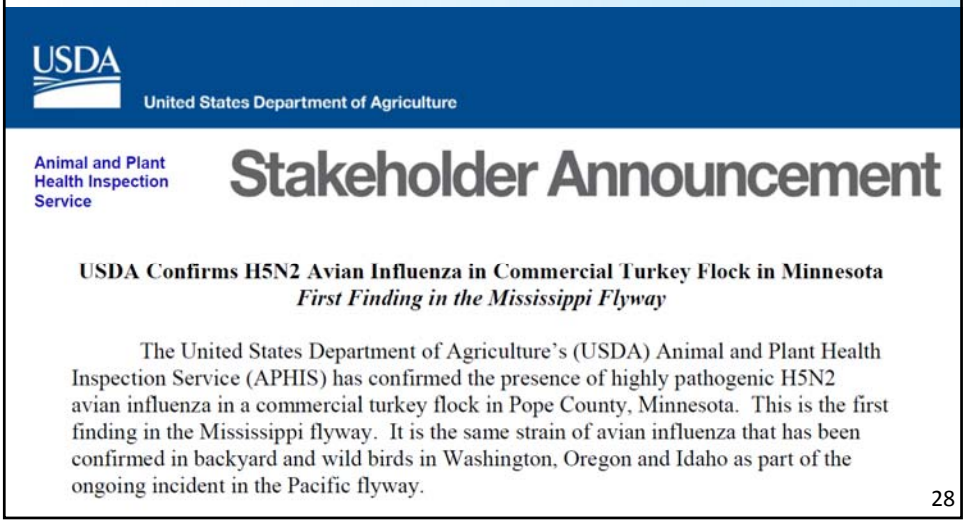
Human Threats Continue to Increase

- 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?

 27

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

- Ground-zero for a future jump to humans?



USDA
United States Department of Agriculture

Animal and Plant Health Inspection Service

Stakeholder Announcement

USDA Confirms H5N2 Avian Influenza in Commercial Turkey Flock in Minnesota
First Finding in the Mississippi Flyway

The United States Department of Agriculture's (USDA) Animal and Plant Health Inspection Service (APHIS) has confirmed the presence of highly pathogenic H5N2 avian influenza in a commercial turkey flock in Pope County, Minnesota. This is the first finding in the Mississippi flyway. It is the same strain of avian influenza that has been confirmed in backyard and wild birds in Washington, Oregon and Idaho as part of the ongoing incident in the Pacific flyway.

28

4/7/15: 8th Confirmed H52N MN Case

MINNESOTA BOARD of ANIMAL HEALTH

- 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

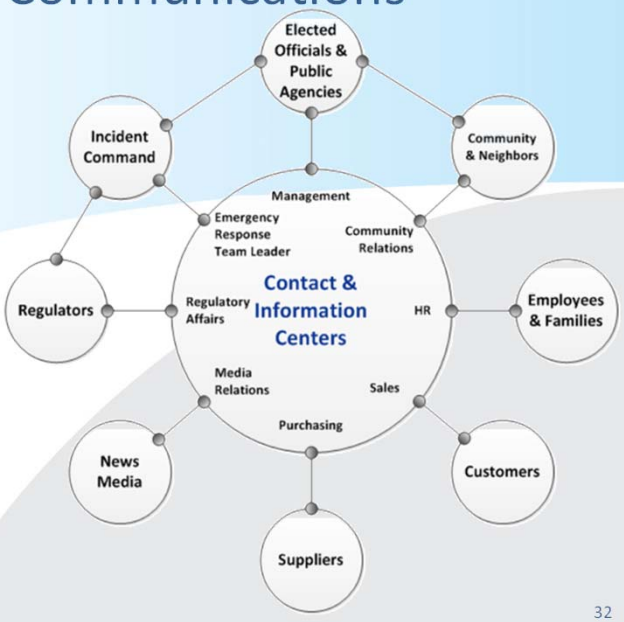
Selected procedures to consider for plan consistency assessments

< --- Time --->

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

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
rptrsmn1@gmail.com
LinkedIn.com/in/RogerPeters1