

SECURE360 conference



ROGER PETERS

AVOIDING DANGEROUS ASSUMPTIONS IN YOUR
BUSINESS CONTINUITY PLANS

MAY 15, 2013 9:45 AM

Roger Peters

Founder, Continuity Onward, Inc.

ContinuityOnward@gmail.com

612-360-3063

Welcome to secure360 2013

- Don't forget to pick up your Certificate of Attendance at the end of each day.
- Please complete the Session Survey front and back, and leave it on your seat.
- Are you tweeting? #Sec360

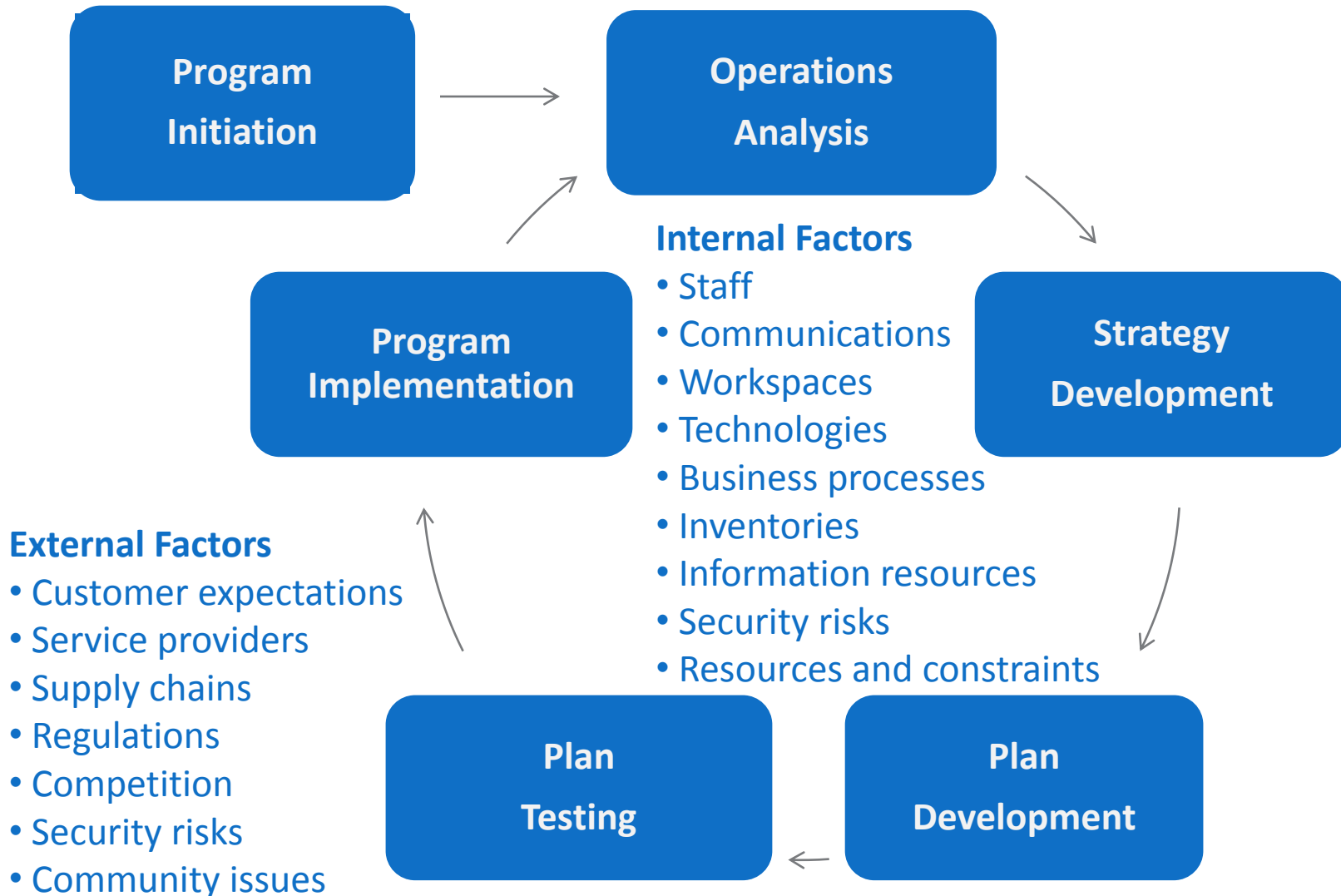
Role of Business Continuity Plan Assumptions

Helps to set boundaries for future plan development and recovery success

- Outline in continuity plans' Executive Summary section
- Use “plan assumptions” versus “plan parameters” due to uncertainties of possible incidents
- Can identify events beyond the plan's probability for successful recoveries
- Helps set responsibility expectations for management and departmental staff
- Can guide future plan enhancement efforts

Business Continuity Planning Lifecycle Summary

The need to document assumptions may be identified throughout the planning life cycle



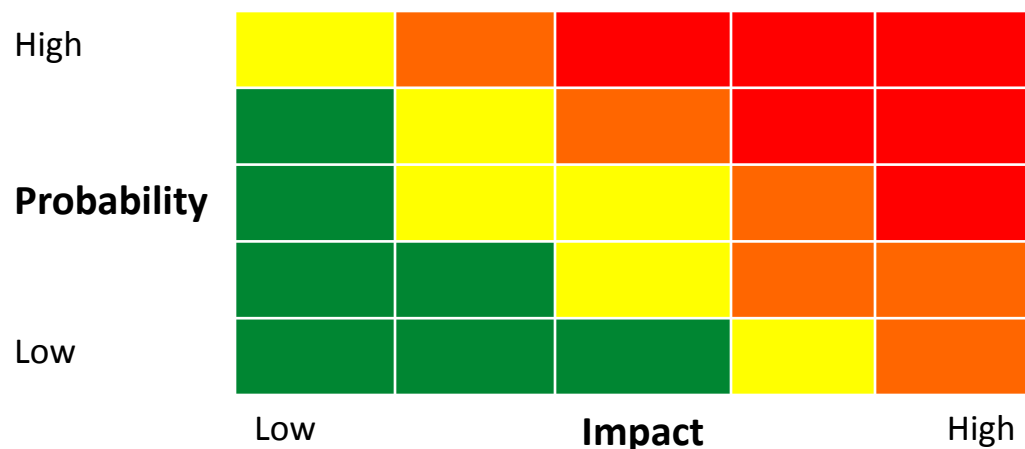
Sample Plan Assumptions

- Sufficient staff are available to perform the critical functions identified in the plan
- Staff can be contacted and are able to report to their designated work locations
- A disaster would not destroy both in-house and hosted systems
- Off-site data back-ups remain secure and can be utilized to restore lost data through the last back-up cycle
- The plan is current and staff have been trained on their recovery responsibilities
- Management will assess the plan procedures and adjust the recovery process as necessary to address the current incident

Conduct Thorough Risk Assessments

Not having a disaster is always the best recovery plan

- Identify where risks and impacts can be mitigated
- Look for “green initiatives” to reduce exposure
- Ask tough questions and consider the “what-ifs”
- Look for risks that may not be adequately considered
 - Don’t miss the “small stuff”
 - Get help if necessary



Accurate Risk Assessment Are Critical

Sample Assessment Excerpts

The facility has:

- A written emergency action plan, in accordance with OSHA...
- Provided state and local authorities the emergency planning and community right-to-know information as required...
- A written emergency response program, in accordance with OSHA...

Safety improvement is an on-going process at the facility. Periodic evaluations are performed to assess the maintenance of safe conditions.

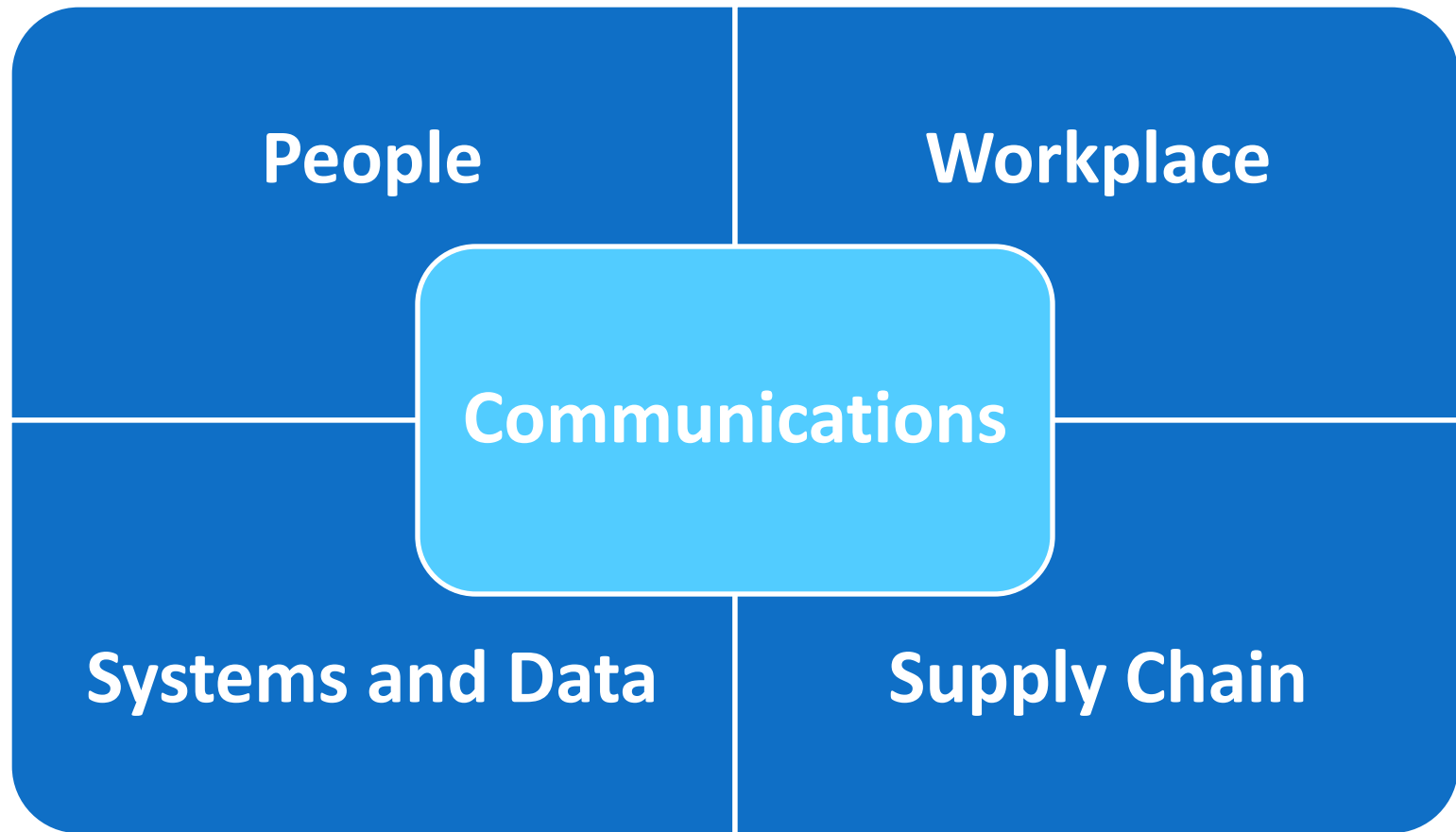
- The company has implemented a prevention program that includes Safety Information, Hazard Review, Operating Procedures, Training, Compliance Audits and Incident Investigation.

Process Flammable Amount Total (lbs) – 0

West Fertilizer filing, 6/30/2011.

Source: 5/10/13, Right to Know Network, rtknet.org

Recovery Requirements





មានបង ការងារកំពុងដំណើរការ
INCONVENIENCE CAUSED IS REGRETTED

Communications Assumptions

Cell phone communications may not be viable during the early recovery stages

- Networks may be impaired or overloaded
 - High call/data traffic levels and/or cell tower damage
 - Text messages are more likely to go through during impaired service
 - Contact your carrier for options if you are part of the nation's critical infrastructure
- Plan Command Center and work space recovery locations in advance to allow initial responses to begin without notification

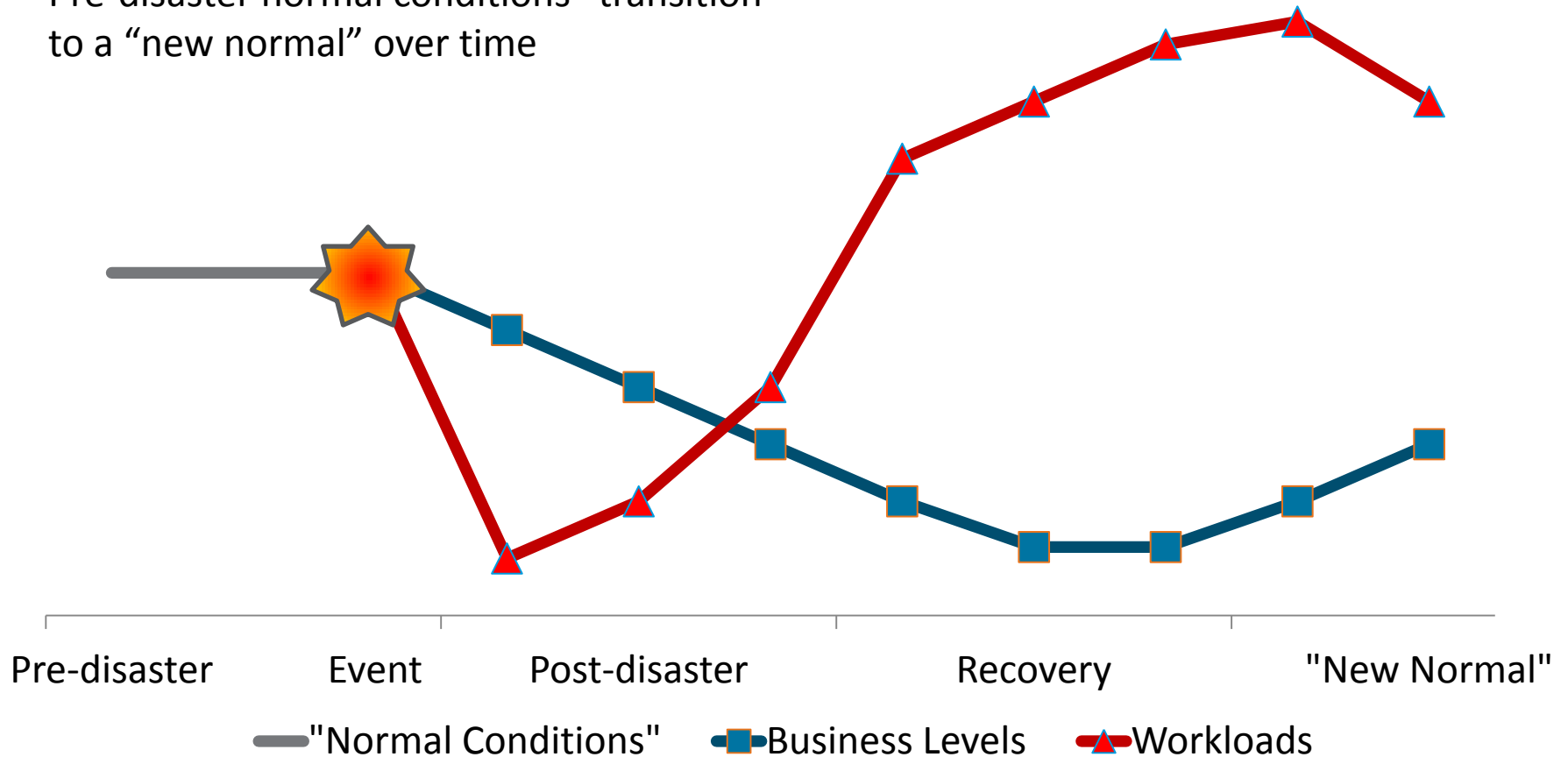
Would your plan work without timely access to the Internet?

Does the plan adequately utilize - and control - social media?

Review Your Workload Assumptions

Example of a possible facility or system disaster
A pandemic would likely reduce workloads

Pre-disaster normal conditions” transition
to a “new normal” over time



Personnel Assumptions

- **Closely review staff impacts from disaster risks**
 - Could an event impact a large number of your staff?
 - Damage to homes from storms or flooding, pandemic outbreak, etc.
 - Are steps required to care for staff, short- and long-term?
 - Can staff effectively connect or interact under all of your high risk/high impact exposures?
- Can staff work effectively from home or an alternate site?
 - Will staff be able to report to an alternate site?
 - Family responsibilities or transportation may create issues
- Has adequate cross-training been performed?
- Do staff know their role in a disaster, including their initial response and processes that must be performed?

Workplace Assumptions

Are adequate seats available for critical departmental functions at a recovery site?

- When can the site be activated?

Can staff work from home?

- Networks may be impaired or overloaded
- Security software or updates may need to be installed
- Can your networks handle high volumes of remote users?
- Departmental operations and dependencies may limit the ability to work remotely
 - Will productivity be reduced at the same time workloads increase due to reduced systems access or staff synergies?

Systems and Data Assumptions

No problem – it's in the cloud

IT providers may not meet your recovery expectations

- Has a realistic recovery simulation or actual recovery been observed and verified?

Systems recovery times may not be as fast as expected

- Are adequate staff available to restore, patch and test all necessary systems within required windows?
- When will the expected recovery clock start?

Data replication may not be as effective as planned

- Could data be your disaster?

Develop Realistic Recovery Times for critical systems and data

- Cover the worst case scenarios, beginning with the time of occurrence

Supply Chain Assumptions

Business as usual for the supply chain during a recovery?

Review your plan's supply chain communications procedures

- Are the impacts of a disaster on the supply chain well understood?
 - What possible exposures are created?
- Are procedures and responsibilities defined for key parties?

Will customers leave if downtime exceeds their expectations?

- Do we know their expectations?
- Will they come back?

Could a disaster create or force contract breaches?

What impact would customer or supplier losses have on our viability?

Recovery Risk Reduction Summary

- Review your risks and business impacts thoroughly
- Don't assume "it can't happen here"
 - Perhaps it just hasn't happened yet
- Watch the human impacts closely
- Ask tough questions throughout the organization
- Offer mitigation strategies appropriate to risk levels and business constraints
- Ensure key processes and temporary operating procedures are adequately defined
- Watch your key vendors' performance and ability to recover within your required windows
- Train staff and test plans
- Communicate, communicate, communicate...

Thank you!

Enjoy the conference

Roger Peters

Founder, Continuity Onward, Inc.

ContinuityOnward@gmail.com

612-360-3063