WOLF
& COMPANY, P.C.

How Technology Companies Can Take BCP to the Next Level

June 19, 2019

Before we get started…

- Today's presentation slides can be downloaded at www.wolfandco.com/webinars/2019
- The session will last about 50 minutes, and we'll then have time for Q & A.
- Our audience will be muted during the session.
- Please send your questions in using the "Questions Box" located on the webinar's control panel.

About Wolf & Company, P.C.

- Established in 1911
- Offers Audit, Tax, and Risk Management services
- Offices located in:
  - Boston, Massachusetts
  - Springfield, Massachusetts
  - Albany, New York
  - Livingston, NJ
- Over 260 professionals

Presenter

Tracy L. Hall, MBCP
IT Assurance Manager
Wolf & Company, P.C
Direct: (413) 726-6884
thall@wolfandco.com

Today's Agenda

- Why Business Continuity Planning (BCP)?
- Current BCP Hot Topics for Tech Companies
- Q & A

The Importance Of BCP

- A recent survey showed that the top causes[1] of downtime were:

– UPS or Hardware Failure	55%
– Human Error	48%
– Cyber Attack	34%
– Software Failure	18%
– Natural Disasters	4%

1 *Percentages are combined across categories*

The Importance Of BCP

- According to Gartner, the average cost of IT downtime is $5,600 per minute. Because there are so many differences in how businesses operate, downtime, at the low end, can be as much as $140,000 per hour, $300,000 per hour on average, and as much as $540,000 per hour at the higher end.

- A study by Data Center Knowledge, comprised of 41 benchmarked data centers, found the average costs of unplanned data center outages include more than $179K in business disruption, a little over $118K in lost revenue and approximately $42K in IT staff productivity.

The Importance Of BCP

- Don’t Let The Door Hit You…
  - 93% of businesses that experience downtime of 10 days or more file bankruptcy within one year
  - 40% of business severely compromised by a disaster go out of business within 6 months

BCP Process

- Business Impact Analysis (BIA)
  - Functions
  - Resource Requirements
  - Business vs. IT Gap Assessment
- Risk Assessment
- Plan Development
  - Introduction
  - Executive Oversight
  - Scope
  - Assumptions and Scenarios
  - Teams/Roles
  - Recovery Strategy

Business Impact Analysis

Business Impact Analysis (BIA)

The process of identifying and prioritizing critical business functions and the resources required to support them into predefined RTOs. Determining RPOs for systems. Should be BUSINESS driven, not IT driven.

RTOs: Recovery Time Objectives

RPOs: Recovery Point Objectives

This exercise is considered **POST** outage.

- Business Functions
- Departments
- Technologies

Risk Assessment

Risk Assessment

The process of identifying the **probability** of specific threats affecting the organization and the **impact** on the organization if they were to occur.

This exercise is considered **PRE** outage.

- Threat Assessment
- Control Assessment

Scenario Based Planning

Worst Case:

Identification of Worst Case type scenario with consideration for other types of incidents

Where Affected?

- Identify the WHERE that will be affected in the scenario

Who Affected?

- Something that affects the company's ability to service customers but does not affect the customers directly

Scenario Based Planning

Incorporating multiple scenarios:

Group threat assessment scenarios by impact:

- Facilities
- Personnel
- Systems

Many scenarios will have multiple impacts

For example:

Fire = potential for Facility, Personnel, and System impact

Personnel Recovery

Have a well thought out and documented strategy for employees:

- Number of required personnel broken down by RTO
- Actual recovery locations
- Ensure proper infrastructure is in place
- Remote work capability?
  - Don’t put all of your eggs in this basket!
  - Power considerations – generators

Team Tasks

Does not matter how many teams are in the BCP, as long as all of the critical tasks are assigned, to include:

- Response and escalation
  - Assessment and declaration
- Technology Recovery
- Business Unit Recovery
- Restoration and return to normal operations

Communications

Creating thorough on-going plans:

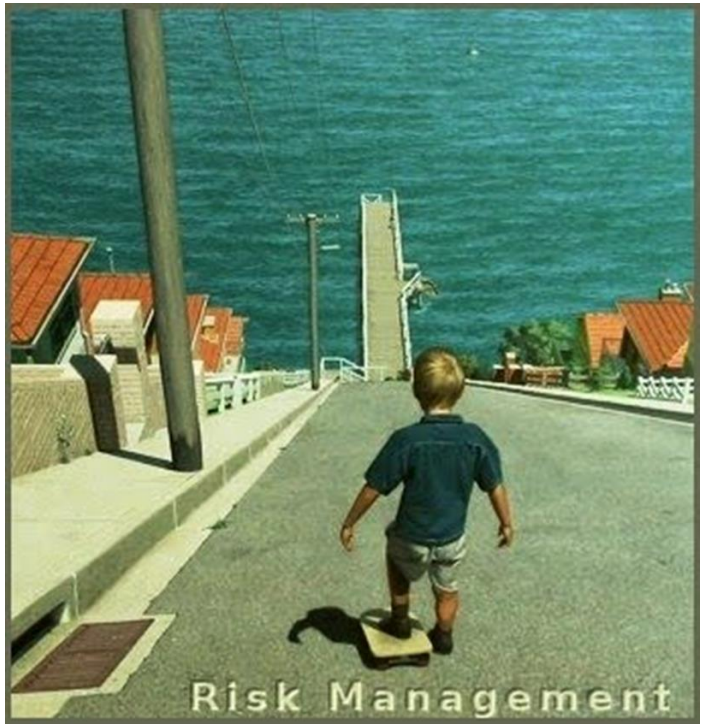
- Not just for onset of incident, but on-going
- Multiple communications vehicles
- Accessibility of contact lists
- Responsibility for initiating communications
- Frequency of contact information updates

Technology Recovery

- Are all critical systems accounted for?
  - Based off the BIA results
- Are adequate resources available for successfully meeting RTOs?
  - Must include infrastructure requirements
  - Adequate hardware and software
  - Sufficient bandwidth
  - Personnel

Outsourcing – what can go wrong?

- Easily disappear
- Give you bad data
- Lose your information
- Cause data security exposure
- Under deliver
- **Be unprepared for a disaster**



Cybersecurity

- Include cyber events in the BCP and Risk Assessment
- Cross reference the BCP and Incident Response Plan
- Incorporate cyber scenarios in testing

Testing

Schedule:

- More frequent, dynamic testing
- Test Plan: Should be multi-year (3 years)
- Rotate technologies of varying criticality
  - Low criticality do not necessarily need to be incorporated
- Must include supporting infrastructure
  - Build into RTOs
- Should be built off of most current BIA (Business Impact Analysis)

Types of Testing

Many ways to achieve “testing”

- **Evacuation Drills**
  - Floor wardens, meeting places
- **Communication Drills**
  - Call Trees
  - Automatic Notification Systems
- **Structured Walkthrough**
  - Smaller groups
  - Review specific details and tasks

Types of Testing

- **Simulation Testing**
  - Who is involved?
    - Experience
    - Authority
  - Incorporates Scenarios
    - Loss of building, technology, people
  - Decision making in a structured environment
  - Roles and Responsibilities
    - Technology
    - Business
  - Tests entire timeline of an event

Types of Testing

- **Technology Test/ Functional Test/ Parallel Test**
  - Roles and Responsibilities
  - Validates RTOs and MADs for technologies that support business functions

    RTOs: Recovery Time Objectives

    MADs: Maximum Allowable Downtime
  - Incorporate internal functions for processing

Ongoing Maintenance

- **BCP Updates should be at least yearly**
  - Employee/Team Members changes
  - Business function changes
  - Technology changes
  - Location changes
  - Third Party Provider changes

Key Takeaways

- Business Continuity Planning involves more than traditional Disaster Recovery Planning which was focused solely on technology
  - People
  - Non technology related resources
  - Communications
  - Third parties
- Outages are caused by a variety of different threats
- Planning does not stop once you've created a plan- maintenance and testing is imperative to ongoing preparedness

Thank you / Questions

Tracy L. Hall, MBCP
IT Assurance Manager
Wolf & Company, P.C
Direct: (413) 726-6884
thall@wolfandco.com