BCP Strategies in a Cloud Environment

Jeremy Sucharski, Director, Armanino LLP

Steve Shofner, Senior Manager, Armanino LLP

Professional Strategies – S32

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

CRISC

CGEIT

CISM

CISA

2013 Fall Conference – “Sail to Success”

Agenda

- Some Basics (Level-Setting)
  - Defining ‘Disasters’
  - Why Plan?
  - Planning Approach
    - Cloud Considerations
  - Testing & Continuous Improvement
- Trends
- ‘Audit Considerations

SOME BASICS
(LEVEL SETTING)

Defining Disasters

Sudden, calamitous event that brings great damage, loss or destruction. (*Source: Merriam-Webster dictionary*)

Natural

- Earthquake
- Flood
- Hurricane
- Drought
- Twister
- Tsunami
- Cold/Heat wave
- Thunderstorm
- Mudslide

Man-Made

- Riots
- War
- Terrorism
- Power outages
- Sprinkler system bursts
- Equipment sabotage
- Arson
- Epidemic
- Pollution
- Transportation accident
- Food poisoning

Technological

- Database corruption
- Hacking
- Viruses
- Internet worms

“DISASTERS” Come in all sizes

Small **Large**

Top Causes and Effects

- Top 3 Causes of Unplanned System Outages:
  - System Upgrades and Patching
  - Power Failure/Issue
  - Fire
- Average Cost of an Unplanned Outage:
  - $287,000

Disaster Recovery Plans vs. Business Continuity Plans

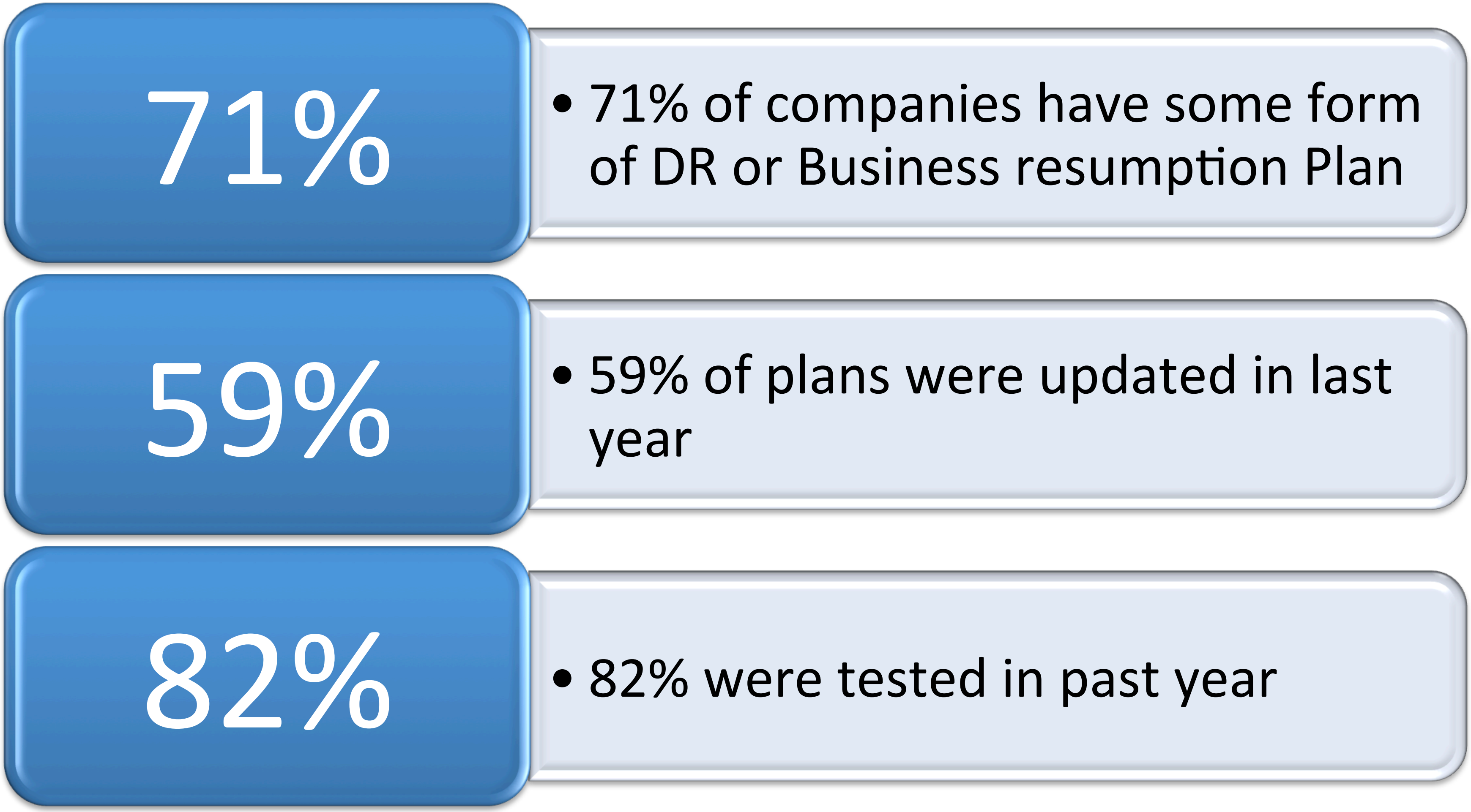
- **Disaster Recovery Plans** – Successfully recover IT systems in the shortest timeframe possible

- **Business Continuity Plans** – Continue critical business functions in the absence of key resources (including people: employees, customers, suppliers, regulators, and others)

Drivers for Having a DRP / BCP

- High availability of data is required by your industry
- Regulatory requirements
- Contractual obligation with a business partner
- It makes good business sense!

Why are DR and BCP Important?



71%

- 71% of companies have some form of DR or Business resumption Plan

59%

- 59% of plans were updated in last year

82%

- 82% were tested in past year

Why are DR and BCP Important?

90%

- 90% of companies who cannot recover operations within 5 days go out of business within 1 year

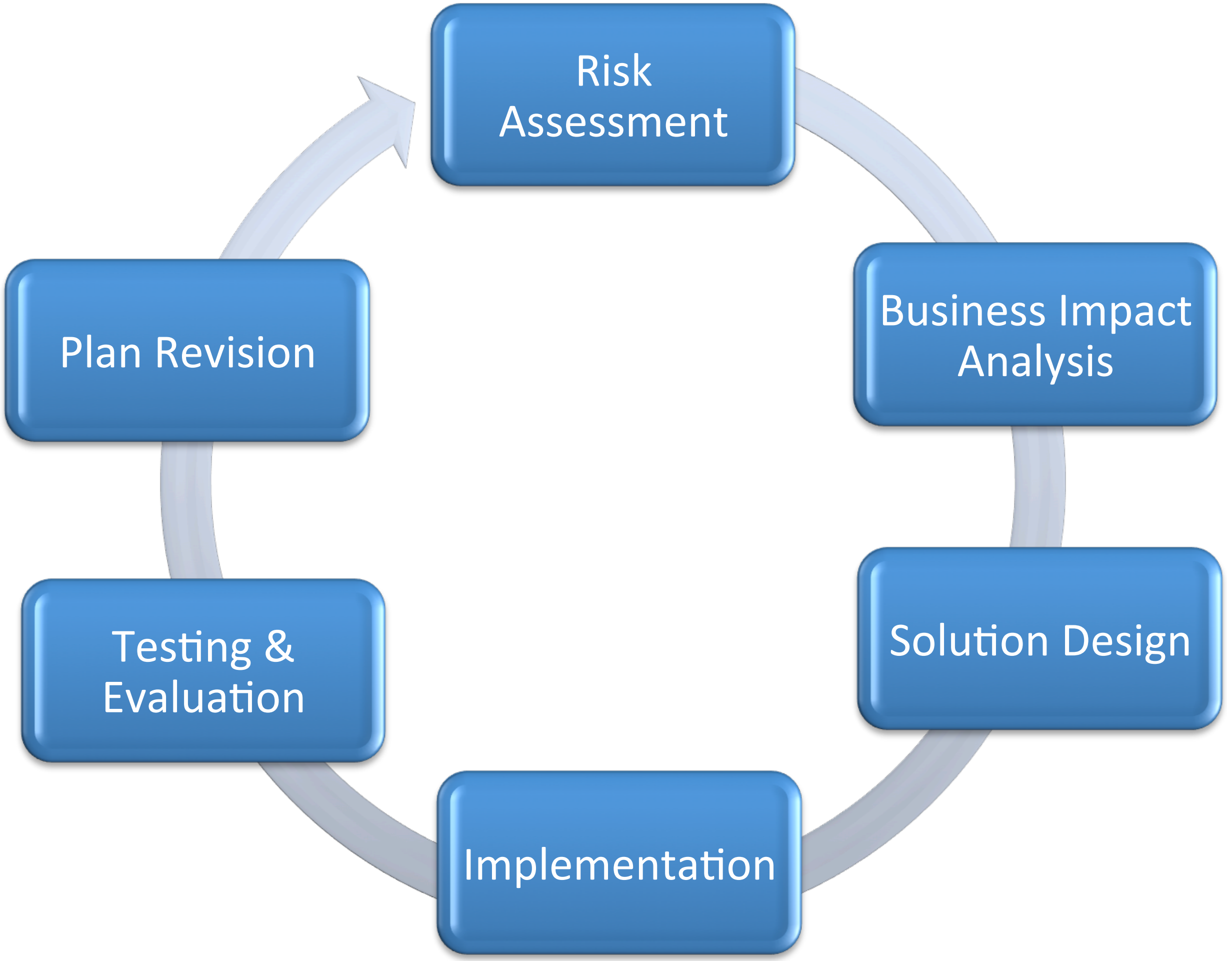
Business Continuity Fallacies

- One Time Event
- Executed in a Vacuum
- Only focused on IT Systems
- An absolute assurance
- Disaster Recovery Planning
- Focused only on large disasters

- An ongoing Process
- Part of the company culture
- Basis For *Reasonable* Assurance of recovery
- Process to mitigate risks that would prevent recovery
- Covering all critical company processes

PLANNING APPROACH

Components of Effective Business Continuity Planning



Conduct a Risk Assessment

Consider the risks to your organization and the probability of each happening:

Natural

- Earthquake
- Flood
- Hurricane
- Drought
- Twister
- Tsunami
- Cold/Heat wave
- Thunderstorm
- Mudslide

Man-Made

- Riots
- War
- Terrorism
- Power outages
- Sprinkler system bursts
- Equipment sabotage
- Arson
- Epidemic
- Pollution
- Transportation accident
- Food poisoning

Technological

- Database corruption
- Hacking
- Viruses
- Internet worms

Common Planning Pitfall

- You do not need to develop individual contingencies for each type of risk/disaster.

- Focus on the absence of key resources, such as (but not limited to) data, regardless of the reason.

Business Impact Analysis Components

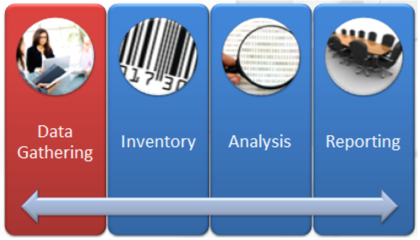
Data Gathering

Inventory

Analysis

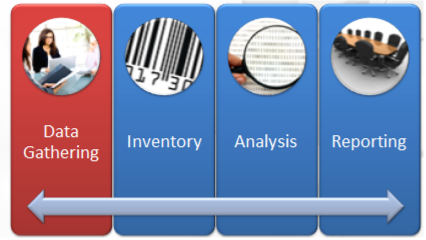
Reporting

Data Gathering



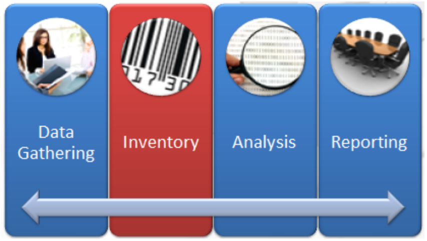
- Begin by “defining” your organization
- Communicate process to entire company
- Identify key individuals to participate in the process
  - – Ensure that this includes a cross section of:
    - Job functions
    - Positions / Levels
    - Responsibilities

Data Gathering



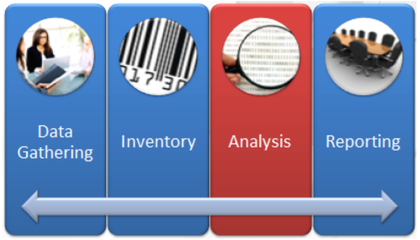
- Develop interview agenda, focused on identifying / understanding:
  - Inputs
  - Process performed
  - Outputs
- Identify key resources, dependencies, and other key considerations:
  - Dependent Applications
  - Related or Dependent Processes
  - Peak Periods/Seasonality
  - Estimated Loss Impact
- Request supporting data throughout
- Gather data for educating company later (supporting your report regarding the impacts to the organization)

Inventory



- Compile what you learned in your interviews and other data gathering
  - Resources
    - Hardware
    - Software
    - Personnel
  - Processes
  - Locations
  - Owners
- "You cant analyze what you haven't discussed."

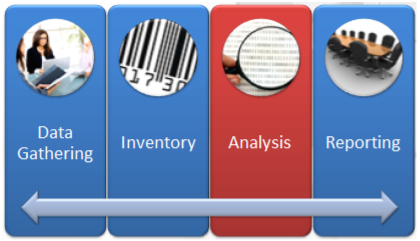
Analyze & Summarize



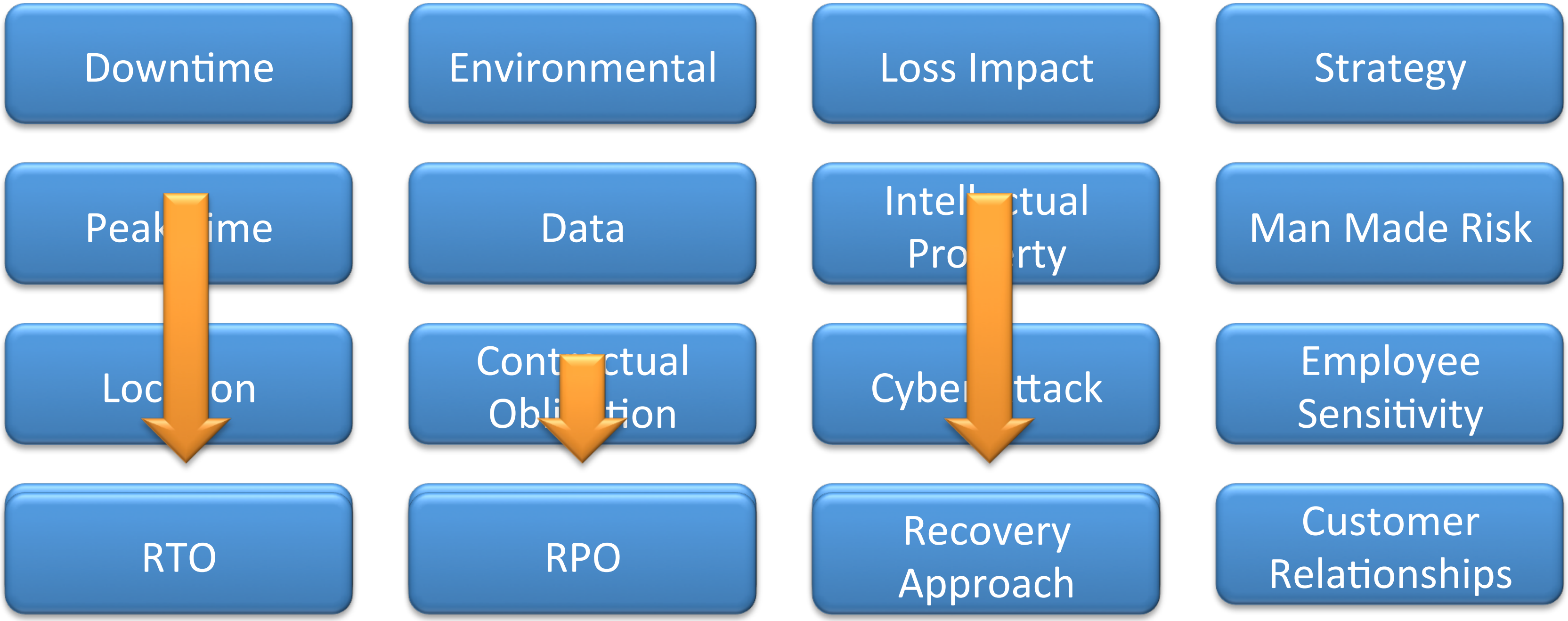
- Identify and prioritize business units, operations, and processes essential to the survival of the business
- Considerations:
  - ✓ Life or death situation
  - ✓ Potential for significant loss of revenue
  - ✓ Obligations to external parties may be jeopardized
  - ✓ Quantify impacts where possible
- Determine:
  - ✓ RTO – Recovery time objectives
  - ✓ RPO – Recovery point objectives

These are critical for determining the order and priority of system recovery

Analysis



- Leverage output from Data Gathering and Inventory Phases
- May include a wide variety of analysis categories including:



Downtime

Environmental

Loss Impact

Strategy

Peak Time

Data

Intellectual Property

Man Made Risk

Location

Contractual Obligation

Cyber Attack

Employee Sensitivity

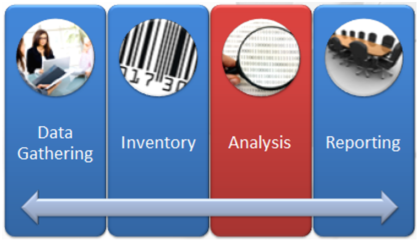
RTO

RPO

Recovery Approach

Customer Relationships

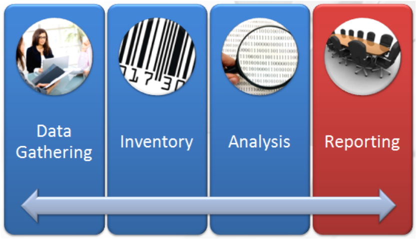
Loss Impact Analysis



Loss Category	Weight	Score (1-5)	Weighted Average	Comments
Financial	68			
Reputation	10			
Client Service	10			
Operational Ability	10			
Safety	1			
Legal & Regulatory	1			

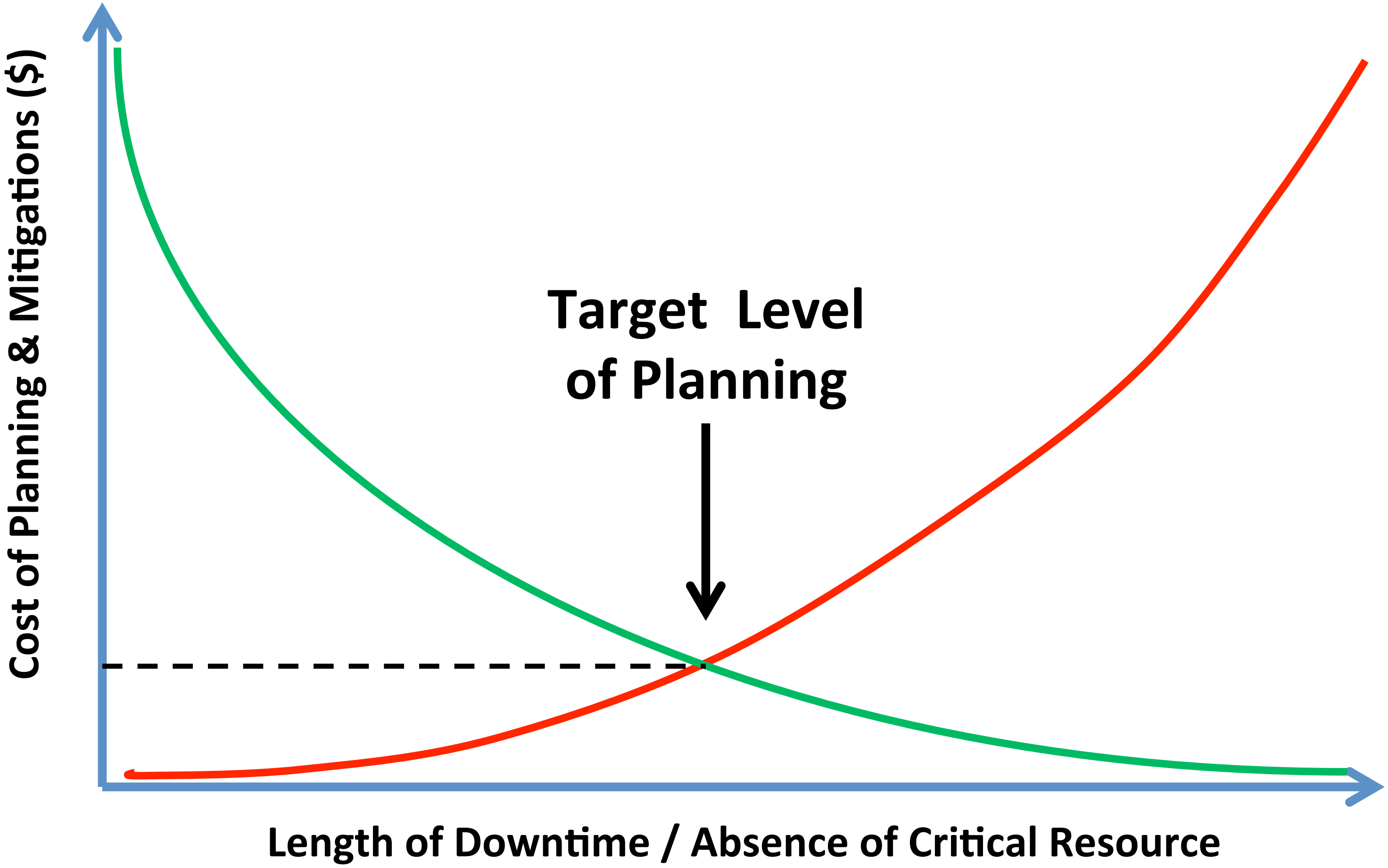
~Example Loss Impact Analysis Criteria Matrix~

Reporting



- Audience
  - Executive
  - Managerial
- Format
  - Include formats that can be leveraged in Solution Design
    - e.g. tables of action items, etc.
- Frequency
  - Initial Reporting
  - Status Reporting

How Much Planning and Mitigation Is Enough?



"Umbrella" Plan Structure
(Common Elements, Regardless of Disaster)

- Assumptions (communications infrastructure in place, primary location still available, primary IT staff available)
- Disaster Management Team (Executives)
- Disaster / Continuity Operation Activities:
  - Detect & Declare Disaster
  - Notify & Convene Disaster Management Team (Establish Command Center)
  - Disaster Management (Command & Control, Status, Communications, etc.)
  - Damage Assessment
  - Equipment Salvage
  - Recovery Processes (alternate site)
  - Continuity Processes (alternate site)
  - Resumption at Primary Site
  - Declare End of Disaster
  - Post Mortem (Lessons Learned)
  - Update DRP / BCP
- Testing & Maintenance

Solution Design

Disaster Recovery Considerations:

Evaluate

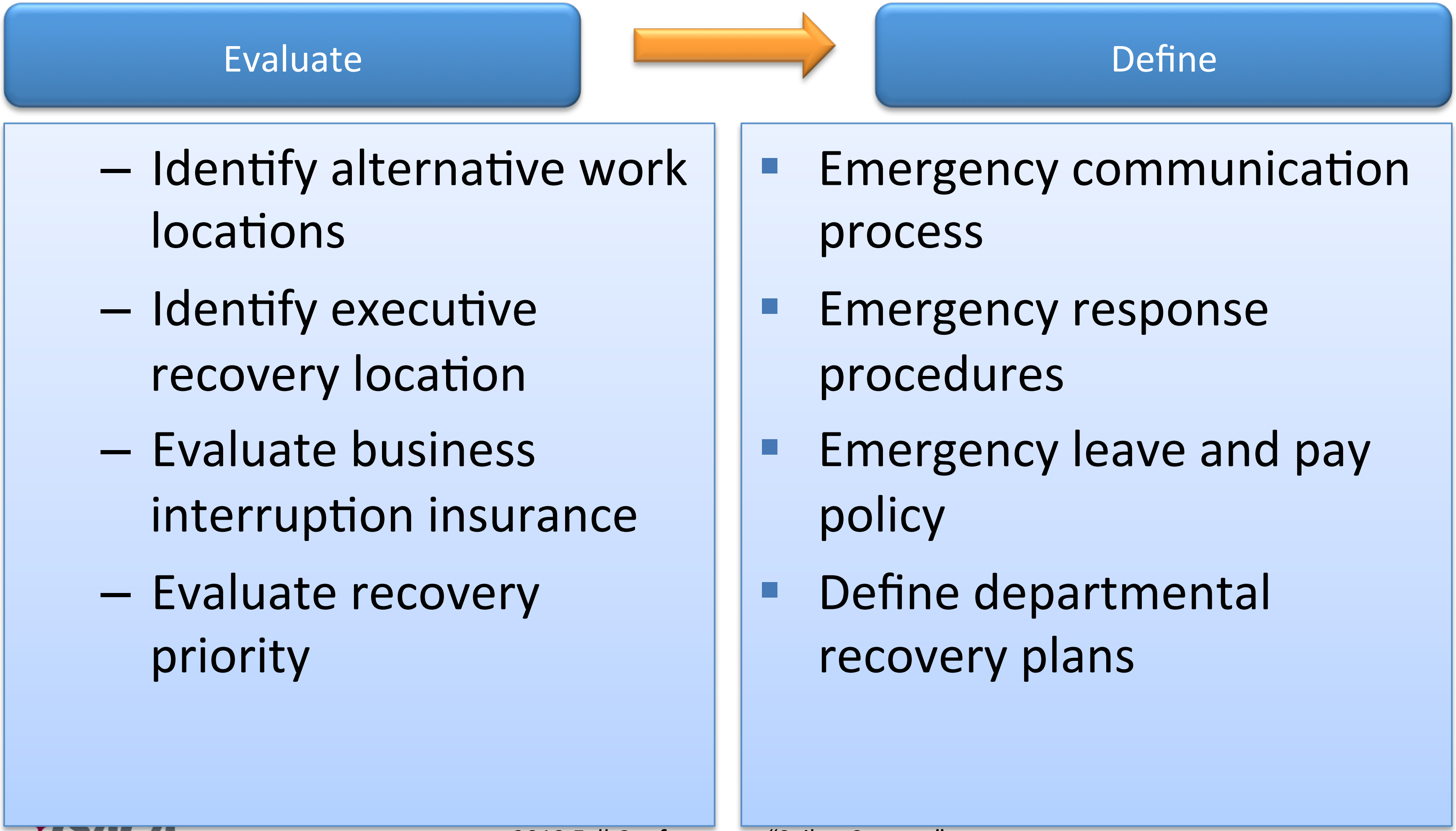
- Evaluate Recovery Strategies
  - Hot
  - Warm
  - Cold
  - Cloud
  - SaaS
  - Reciprocal agreements
  - Local
  - Geographically Separate
- Identify Primary and Recovery Locations
- Translate recovery requirements into actions for IT

Define

- Define recovery approach
- Form recovery team
- Document and Communicate Implementation Plan
- Fold into existing IT plans (if possible
- Leverage SME's
- Categorize Tasks/Effort:
  - Technology
  - Process
  - Training and Education

Solution Design

Business Continuity Considerations:



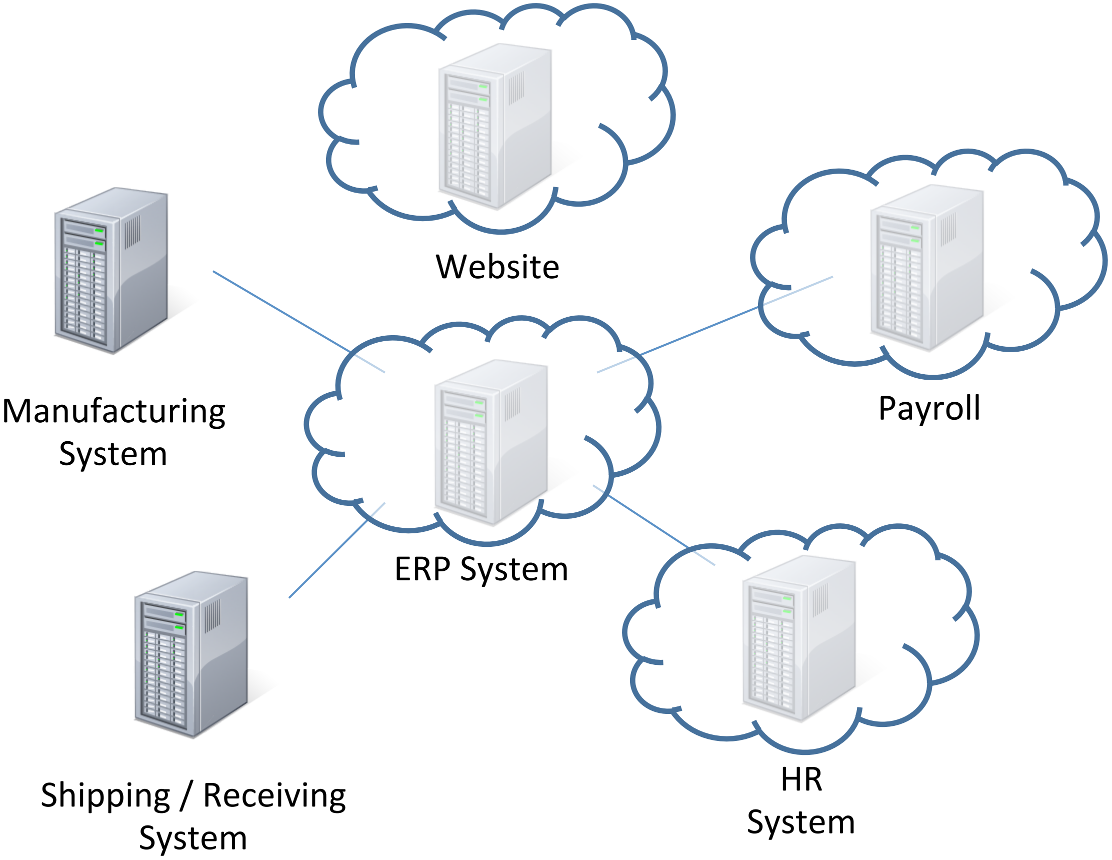
Evaluate

- Identify alternative work locations
- Identify executive recovery location
- Evaluate business interruption insurance
- Evaluate recovery priority

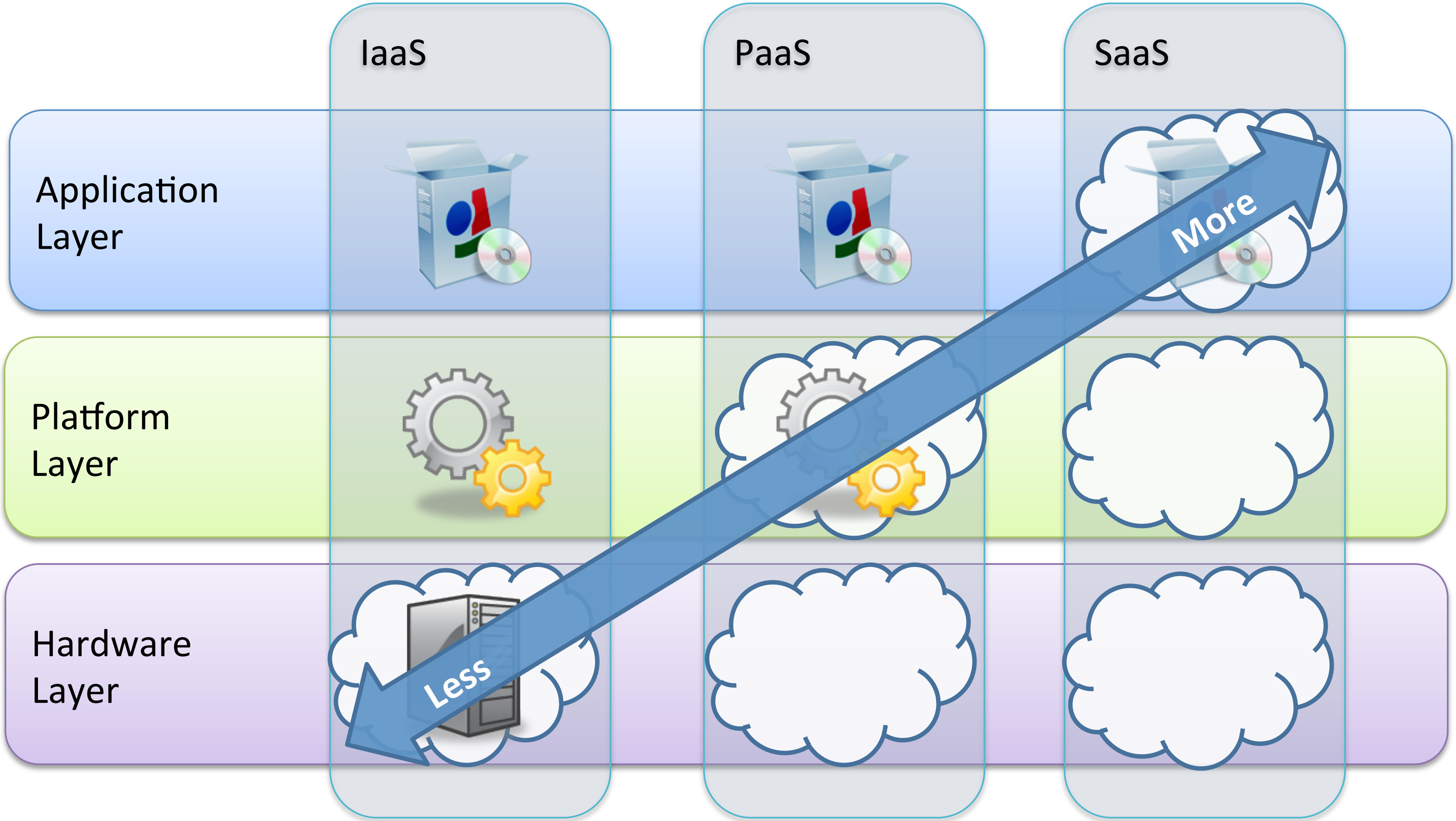
Define

- Emergency communication process
- Emergency response procedures
- Emergency leave and pay policy
- Define departmental recovery plans

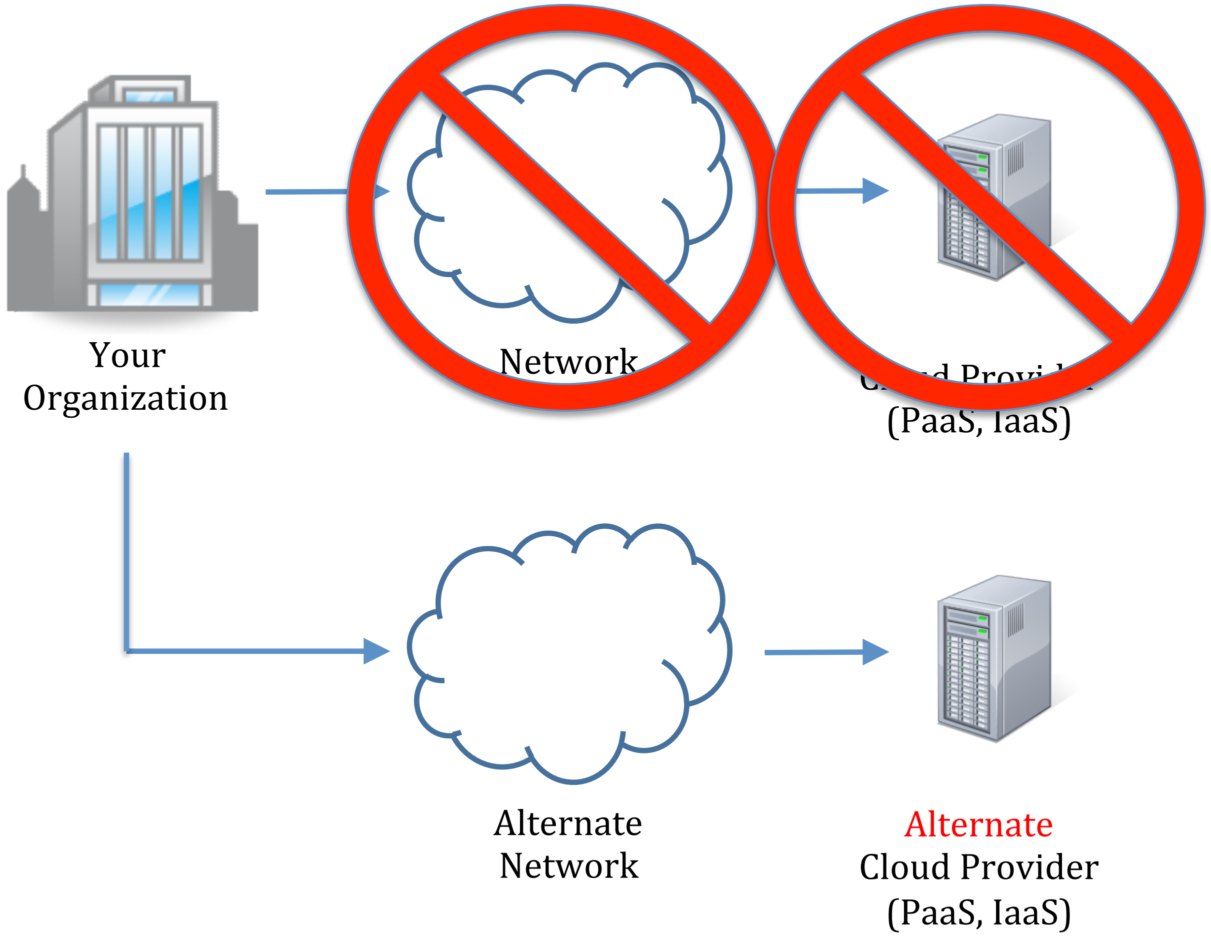
Solutions For Cloud Apps



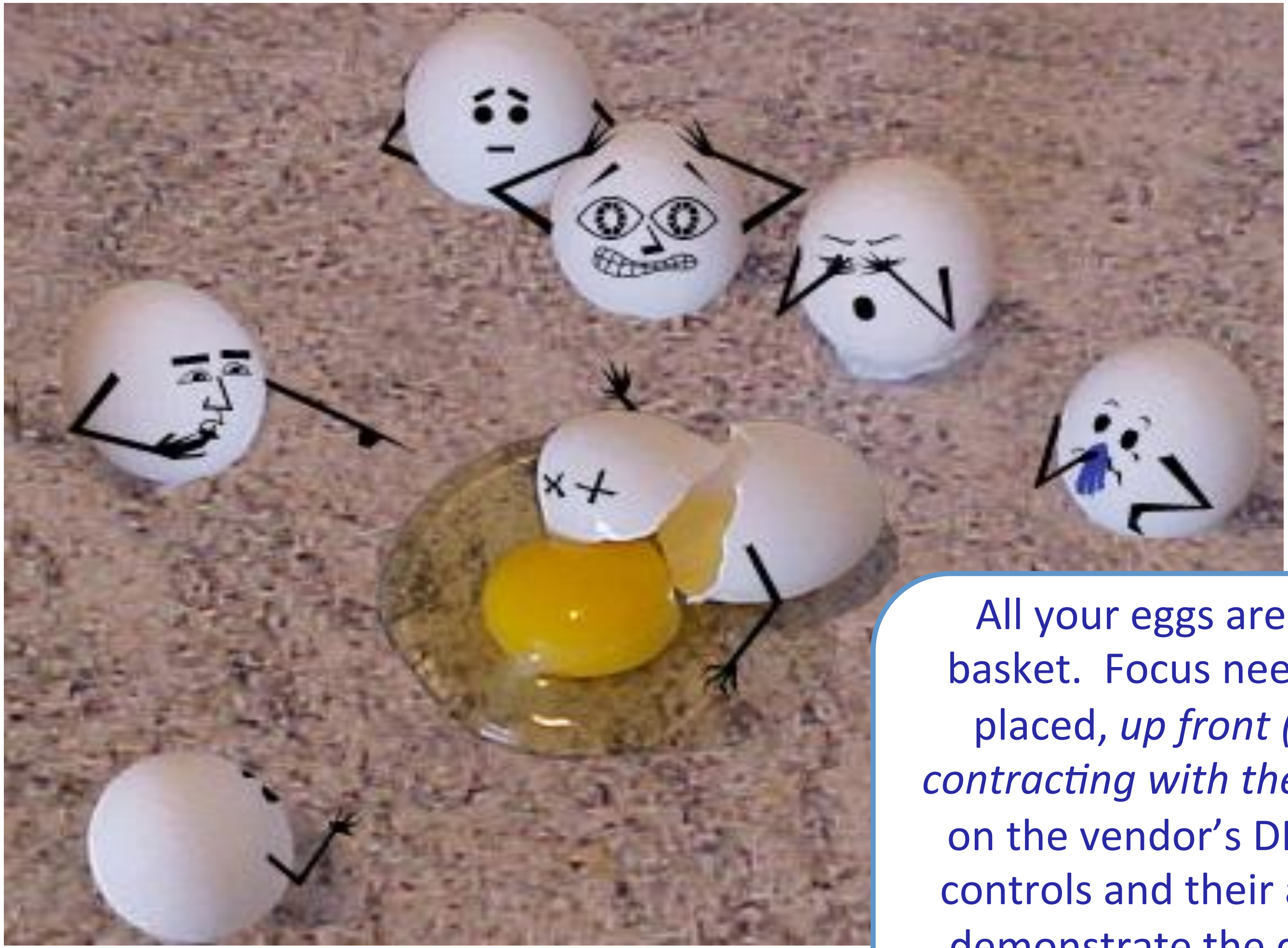
IaaS, Paas, Saas, & Reliance on Vendors



IaaS & PaaS DRP / BCP Strategy


Your Organization
Network
Cloud Provider (PaaS, IaaS)
Alternate Network
Alternate Cloud Provider (PaaS, IaaS)

SaaS DRP / BCP Strategy

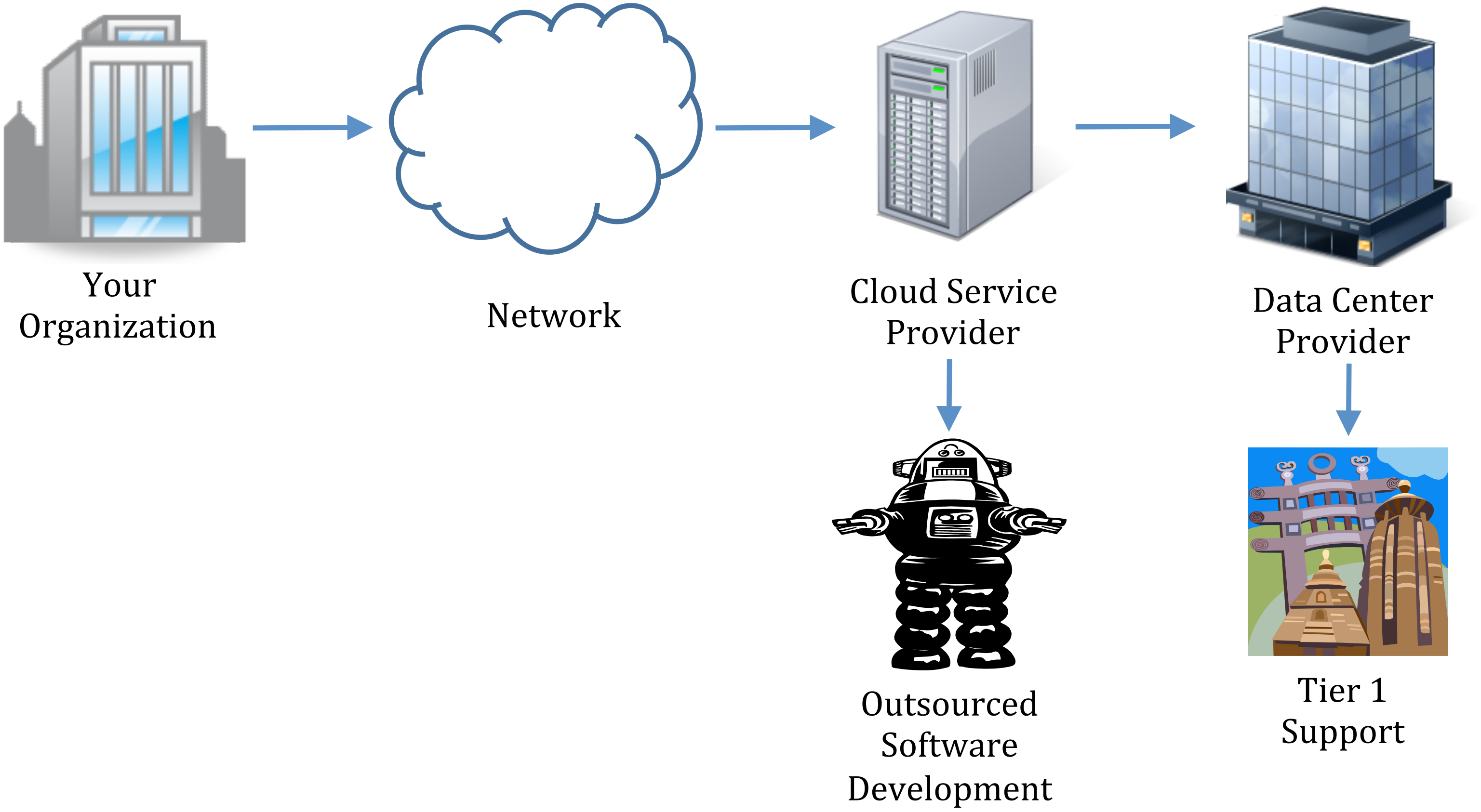


All your eggs are in one basket. Focus needs to be placed, *up front (before contracting with the vendor)*, on the vendor's DRP / BCP controls and their ability to demonstrate the controls' ongoing effectiveness.

Cloud Consideration Summary

- If you contracted for an IaaS or PaaS service, plan for redundancy by contracting with more than one vendor
- If you contracted for a SaaS service:
  - Understand the vendor's environment
  - Understand the vendor's disaster recovery / business continuity plan
    - **BEWARE:** BCP / DRP is often separate from Service Level Agreements (e.g., guarantees of 99.999% uptime). Most SLA's also have a force majeure ('acts of God') clause. Understand what guarantees they provide regarding disaster situations.
  - Ensure ongoing compliance
    - Obtain and *review* a Service Organization Controls (SOC) report
    - Ensure there is an audit clause in your agreement

‘Nested’ Cloud Services

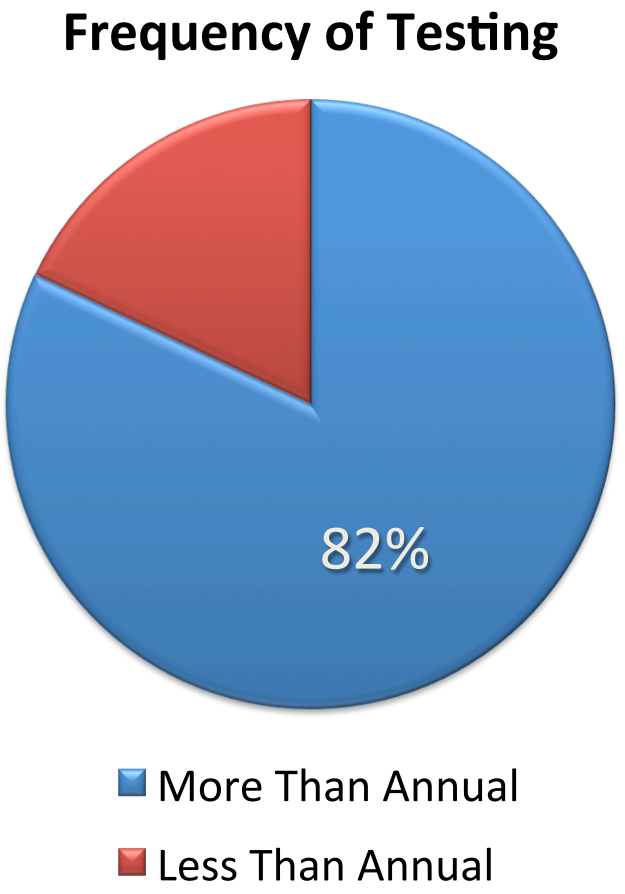


General Considerations

- Key staff (and/or vendors) may or may not be available during the recovery effort
  - Plan for Primary, Secondary, Tertiary, others
  - Ensure adequate decision-making and spending authority in advance
- Communications and infrastructure for the region may/may not be functioning
- Escalation plan and related timelines
- Recovery procedures should provide enough detailed so that alternate resources can follow if needed
- Recover all vs. subset of the required systems to meet critical (not all) business processes
- There will be performance degradation
- Functionality may be limited

Testing & Improvement

- Test Your Plan
  - What % of companies test their DR or BCP plans more than annually?

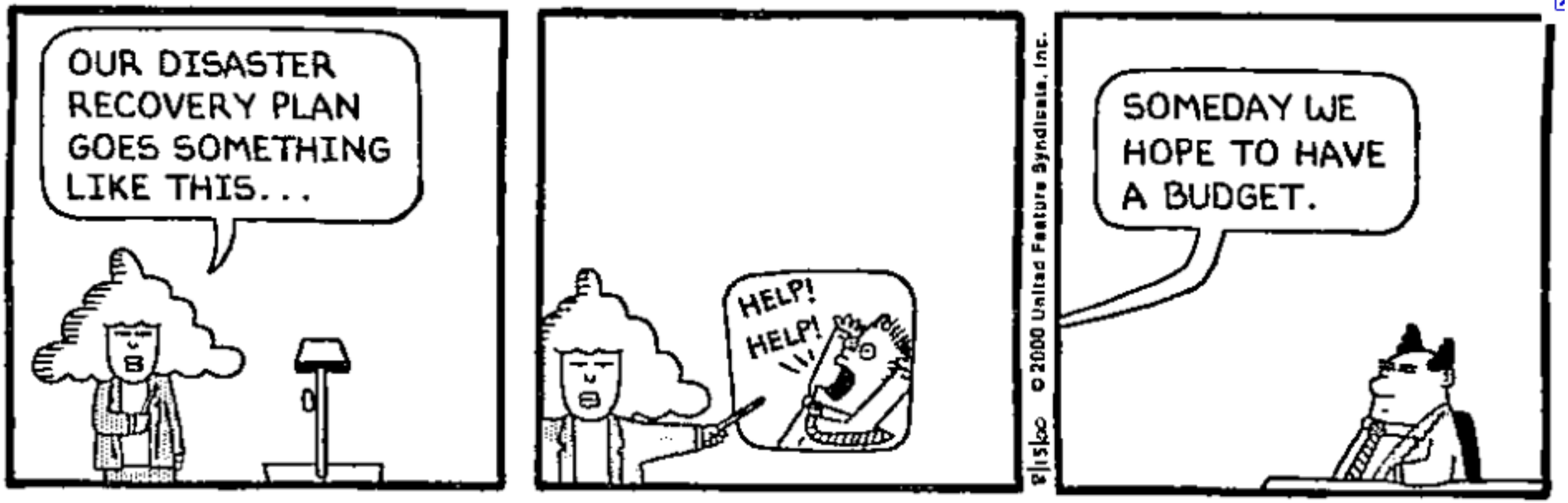


Testing & Improvement

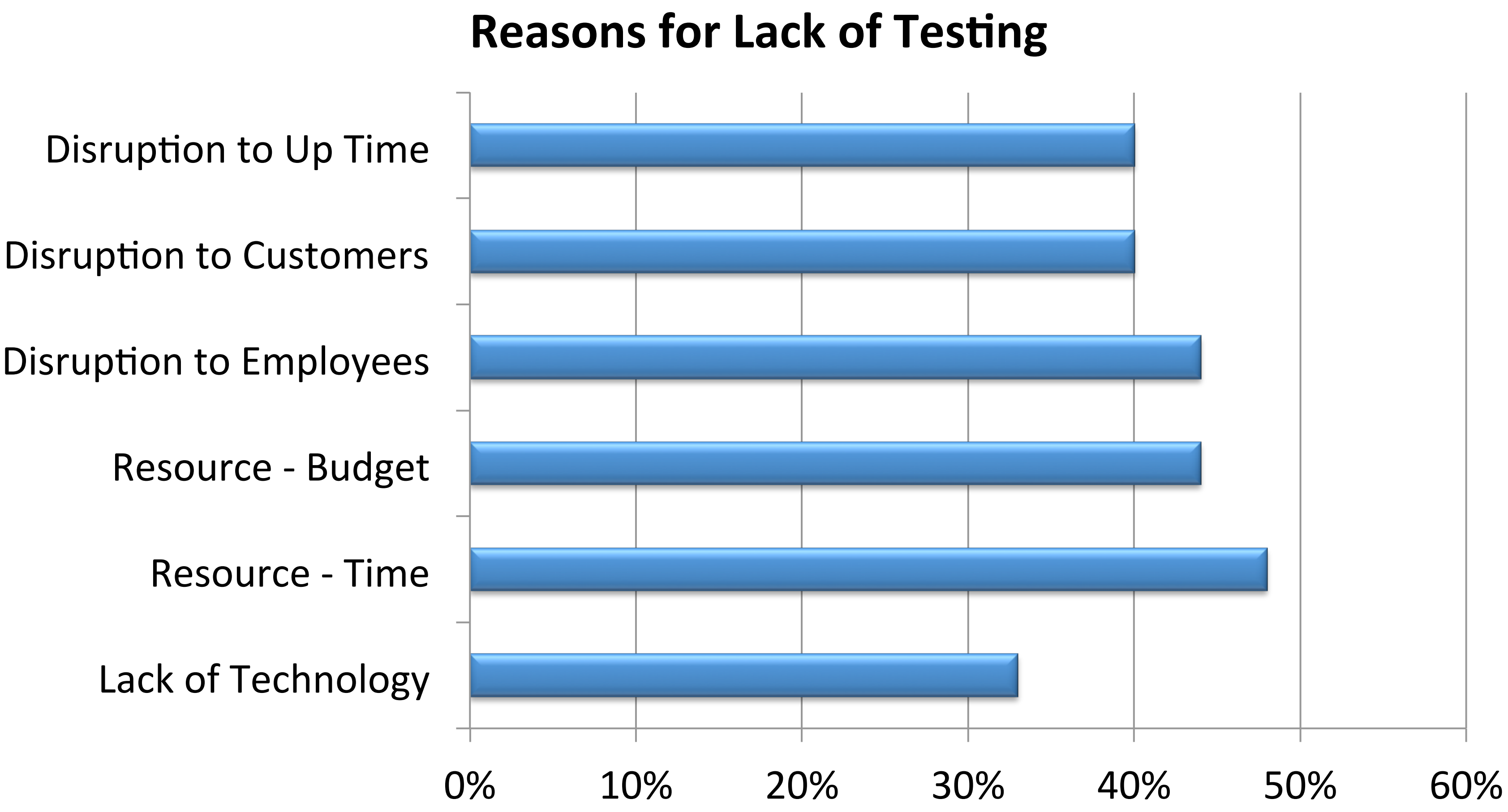
- Types of Testing:
  - Table Top Testing
  - Crisis command team call-out testing
  - Fail Over Testing
  - Technical swing test from primary to secondary work locations
  - Technical swing test from secondary to primary work locations
  - Application test
  - Business process test
  - Full Recovery Exercise
- Debrief & Discussion after Testing

So Why Skip The Testing?

- Testing type and depth is highly variable
- 18% of companies reported that did no DR or BCP Testing


OUR DISASTER RECOVERY PLAN GOES SOMETHING LIKE THIS...
HELP! HELP!
© 2000 United Feature Syndicate, Inc.
SOMEDAY WE HOPE TO HAVE A BUDGET.

So Why Skip The Testing?



Continuous Improvement

- Plan Revision
  - Evaluate Plan Assumptions and Test Results
  - Re-conduct selection of BIA Interviews
  - Update system inventory
  - Update hardware inventory
  - Determine what plan execution steps require revision
  - Revise and publish
- Ongoing Training
  - BCP Leaders
  - Company SME's
  - End User Updates (*including Audit Committee and BOD*)

Trends

- BCPs are the #2 area of increased IT Spending
- Increased Focus at C-Suite
  - Driven by:
    - Strategy
    - Compliance
    - Business Environment
- Integrating BCP, ERM and Risk Assessment

Trends

- Virtualization
- Cloud
- Mobile
- Social Media
- BYOD
- Big Data
- ISO 22301

Keys To Success

- Start Early
- Attack the issue as a Business problem…not an IT problem
- Focus strong attention on the BIA
- Maintain traction after BIA
- Test and Revise

Audit Considerations

- DRP / BCP Team Organization and Communication
  - Secondary, Tertiary, etc. Identified and Empowered
- Risk Assessment
- Business Impact Analysis
  - RTOs, RPOs, etc.
- Cloud Vendors
  - Disaster clauses (may be separate from SLAs)
  - Service Organization Controls (SOC) Reports obtained and reviewed regularly

Audit Considerations (continued)

- Documentation and Distribution
  - No single point of failure (everything in one location)
  - Includes all phases identified above (declaration, damage assessment, salvage operations…declare conclusion of disaster operations, resume normal operations, perform 'post mortem' meeting, improve plan)
- Testing
  - Frequency
  - Type
  - Results
- Maturity Assessment

Resources

- NIST Contingency Planning Guide for Federal Information Systems http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf
- Disaster Recovery Journal – drj.com
- Business Recovery Manager's Association – brma.com
- DRII the Institute for Continuity Management – drii.org

Presenters

Jeremy Sucharski, CISA, CRISC

JeremyS@amllp.com

925-790-2838 (office)

510-331-0940 (cell)

Steve Shofner, CISA, CGEIT

Steve.Shofner@amllp.com

415-790-2879 (office)

510-681-6638 (cell)

APPENDIX

IMPORTANT PHASES OF DISASTER OPERATIONS

Roles and Responsibilities

The Disaster Recovery Team includes…

Disaster Recovery Coordinator

- C-level individual or manager who directs the teams and serves as the leader of the recovery efforts

Media/Communications Representative

- C-level manager, legal counsel or similar spokesperson who ensures a consistent message is communicated to the media

Salvage Team

- IT and business unit staff who assess the equipment to determine if damage is minimal or extensive, and if new equipment needs to be procured

Recovery Team

- IT team responsible for system rebuilding and data restoration

Backup Support Staff

- The secondary individuals who can assume the role of the primary who may not be available

Declaration of a Disaster

- Criteria for invoking the disaster recovery plan
  - ✓ Severe disruption to service
  - ✓ Potential for major data loss
  - ✓ Data security may have been compromised
- Initiating the call tree process
  - ✓ Disaster Recovery Coordinator starts the notification and activates the other teams involved in the recovery effort
  - ✓ Business unit managers responsible for notifying their teams

Get the word out!

- Key Stakeholders:
  - Customers
  - Employees
  - Suppliers
  - Insurance providers
  - Civic agencies (e.g., Police, Fire, National Guard)
  - Regulators
  - Local media

- Communication Channels:
  - ○ Intranet
  - ○ Externally-hosted website (consider mobile)
  - ○ Phone
  - ○ Automated phone service (call-out, dial-in, or both)
  - ○ Print media
  - ○ Mail
  - ○ Bulletin board

Disaster Recovery Activities - Equipment Salvage

- Primary site may be available, but access is restricted due to danger
- Survey damage to assets for insurance purposes
- Determine if anything can be saved or serviced by the vendor immediately
- Device/Server support agreements need to be leveraged
- Test potentially damaged systems before relying on them for recovery operations
- Initiate emergency procurement process for immediate hardware, software, and appliance needs

Disaster Recovery Activities - System Recovery Process (Alternate Site)

- IT team members are heavily involved with assistance from various operations teams depending on system being recovered
- Rebuild (makeshift) network, ensuring security from Internet-based threats
- Think about connections that need to rerouted or pointed to recovery site
- Acquire or rebuild server hardware and install base operating system and patches
- Install and configure application and database software
- Consider controls (IT and non-IT)
- Configure accordingly and test
- Initiate data restoration process
- Test processing functions with business unit representatives
- Get satisfactory response before deeming system operable and live in the recovery environment

Disaster Recovery Activities - Resumption at Primary Site

- Primary site has been declared safe by Fire Department, inspectors, other officials
- Connections to Internet and WAN have been re-established
- Replicate data back or move the recovery system for use as the primary system
- Re-establish connections or DNS pointers to primary site
- Test functionality with business process owners and get satisfactory response

Business continuity

- Questions:
  - How will you continue delivering your process/service?
  - How will you manage employees (e.g., payroll)?
  - How will you manage vendors?
  - Others?
- Considerations:
  - Alternate manual/paper-based methods
  - Alternate controls (Financial, Operational, ITGCs, Security, etc.)

Declaring the End of the Disaster

- Communication to media, business partners, clients, other stakeholders
- Debrief with disaster recovery team members on what was good and where improvements need to be made
- Update the disaster recovery plan with new lessons learned

Key Considerations

- Human safety is #1
- Data security
- Remote work access
- Equipment acquisition
- Media storage
- DNS
- Sufficient insurance