Business Continuity Trends & Best Practices Workshop

Raymond Kettner, CBCP
Manager, Business Continuity Consulting
HP Services Business Continuity Services - Americas

Objective

Provide an understanding of…

- What is Business Continuity, High Availability, & Disaster Recovery

- Importance of using risk mitigation planning, maintenance and applying lessons learned

Offer suggestions & tools to…

- determine what is needed for your business.

Key concepts and terms

What is business continuity?

It is…

- A way of doing business and continuing to stay in business
- A plan to assure business processes
- An integrated approach to link IT availability management and continuity and recovery
- An on-going effort to improve IT service levels and availability

It isn't…

- A specific product or technology or a service
- A "project" with a beginning and an end
- Just disaster recovery or high-availability

Business drivers

Stricter business requirements

- Growing regulation
  - –Sarbanes-Oxley
  - –HIPAA
  - –SEC
- Competitive advantage
- Quality, efficiency & dependence on e-business

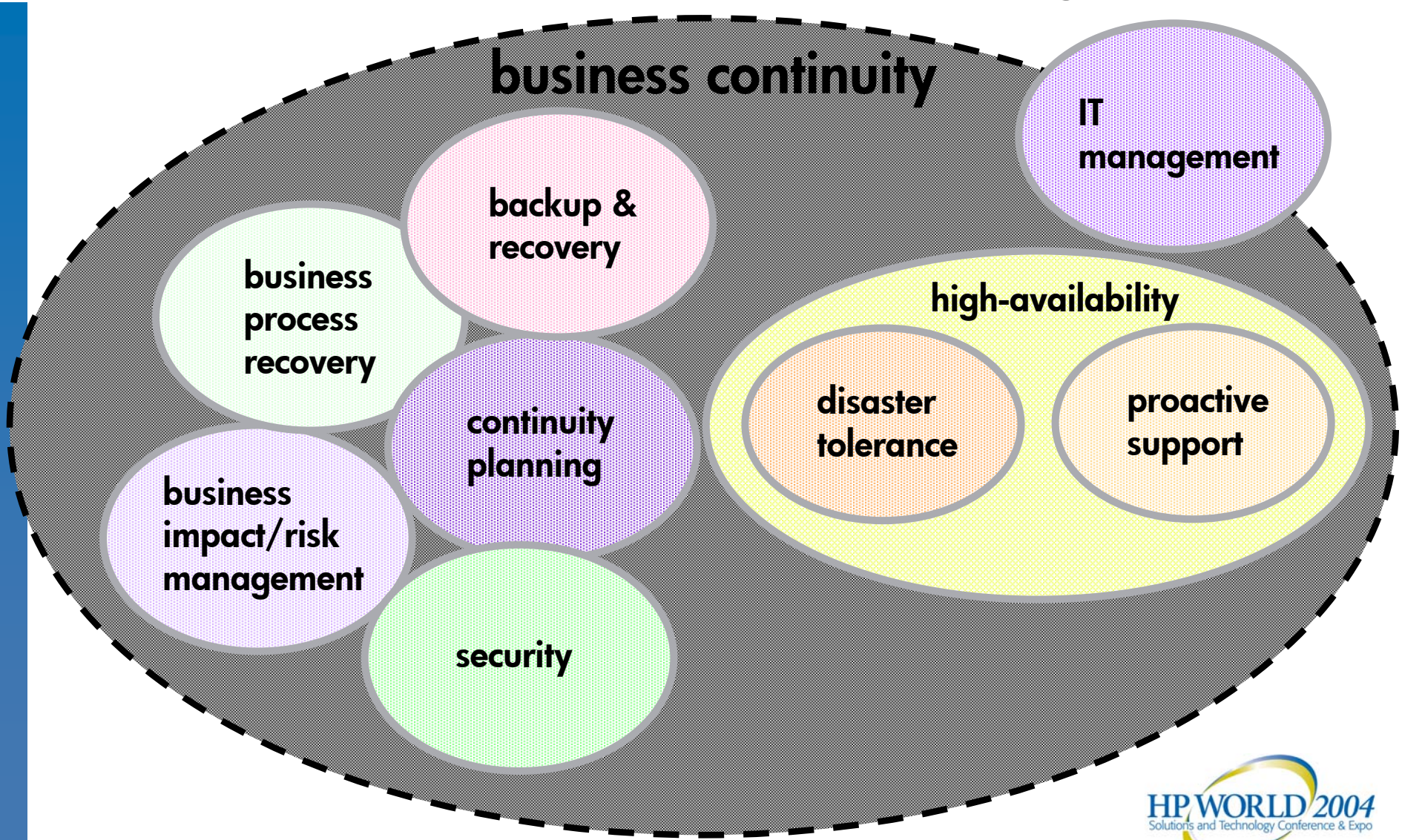
New business models

- Reliance on IT
- 7x24 operations
- Planned downtime no longer acceptable
- Smaller recovery windows
- SLA penalties
- Resilient operations

Increased need for business protection

- Revenue
- Productivity
- Fines and penalties
- Goodwill
- Employee morale
- Due diligence

Terminology:
some definitions and how they work together



Business continuity planning vs. IT continuity planning

Business Continuity Planning (BCP)

A Business Continuity Plan allows you to plan for critical business processes that require people, office supplies and tools, along with key business functions and suppliers that will be needed during a disaster or extended outage.

IT Continuity Planning

An IT Continuity Plan allows you to plan for critical IT components, tools, support staff and the IT infrastructure along with key processes and suppliers that will be needed during a disaster or extended outage. An IT Continuity Plan is an attachment to a BCP or can be built in as part of the BCP.

Critical IT recovery terms

Maximum Tolerable Outage (MTO):

Window of time from the start of an event/outage to when the impact on the business becomes too great, causing damage to the business's reputation and/or revenue.

Recovery Time Objective (RTO):

Window of time from a declared disaster to when impact on the business becomes too great causing damage to the businesses reputation and/or revenue.

Recovery Point Objective (RPO):

Point in time at which data is recovered or restored. Considered a measure of allowable data loss

Escalation and Fix Window:

The MTO – RTO = Escalation/fix window. Time from an outage to time when a disaster declare decision should be made.

Business Impact Analysis (BIA):

Process of analyzing all business functions and the effect that a specific disaster may have upon them. This process determines the MTO, Fix window, RPO & RTO.

Lessons learned and best practices

best practices: analyze

- ✓identify & minimize business risks and exposures & assess level of readiness for recoverability and resumption
- ✓define criteria for classifying business processes (vital, critical, important, deferrable)
- ✓identify financial (tangible) and operational (intangible) business impact of downtime in order to define recovery time objectives (RTO) and recovery point objectives (RPO)
- ✓gain validation and support from business units

How do you build enforceable IT continuity plans?

Have professionals that can help you:

- Understand your risks
- Determine what IT components are critical to reputation and revenue
- Build recovery strategies that meet RTOs and reduce risk
- Write and document IT continuity plans
- Train staff to invoke IT continuity plan
- Train staff to recover within defined RTO window
- Manage rehearsals to ensure plan is invokeable and provide continuous training
- Maintain plan as a living document

What kind of issues make it hard to recover in the right RTO?

1. Do you understand what IT members you need on each team in a disaster?
2. Are your teams trained to recover each critical IT component?
3. Do your team members understand the declare process?
4. Are your managers trained to become the Disaster Management Team and trained to run and manage a command center?
5. Do you have a Crisis Management team that reports status and escalates issues to key corporate management?
6. Does your IT staff understand Recovery Time Objectives for all critical IT components?
7. Does your IT staff know where to report, by phone or in person, when an outage occurs that renders the production site unavailable?
8. Does your staff understand Life Safety? When and when not to report?
9. Do your teams understand who to pass the baton to and when to pass the baton?
10. Do your IT teams understand when to escalate for help and how to escalate?

Common Mistakes

- Trying to anticipate the future based upon recent events
- Not identifying which app's end-users consider mission-critical
- Conducting rehearsals that aren't realistic
- Only thinking about IT
- Overlooking people that run the equipment

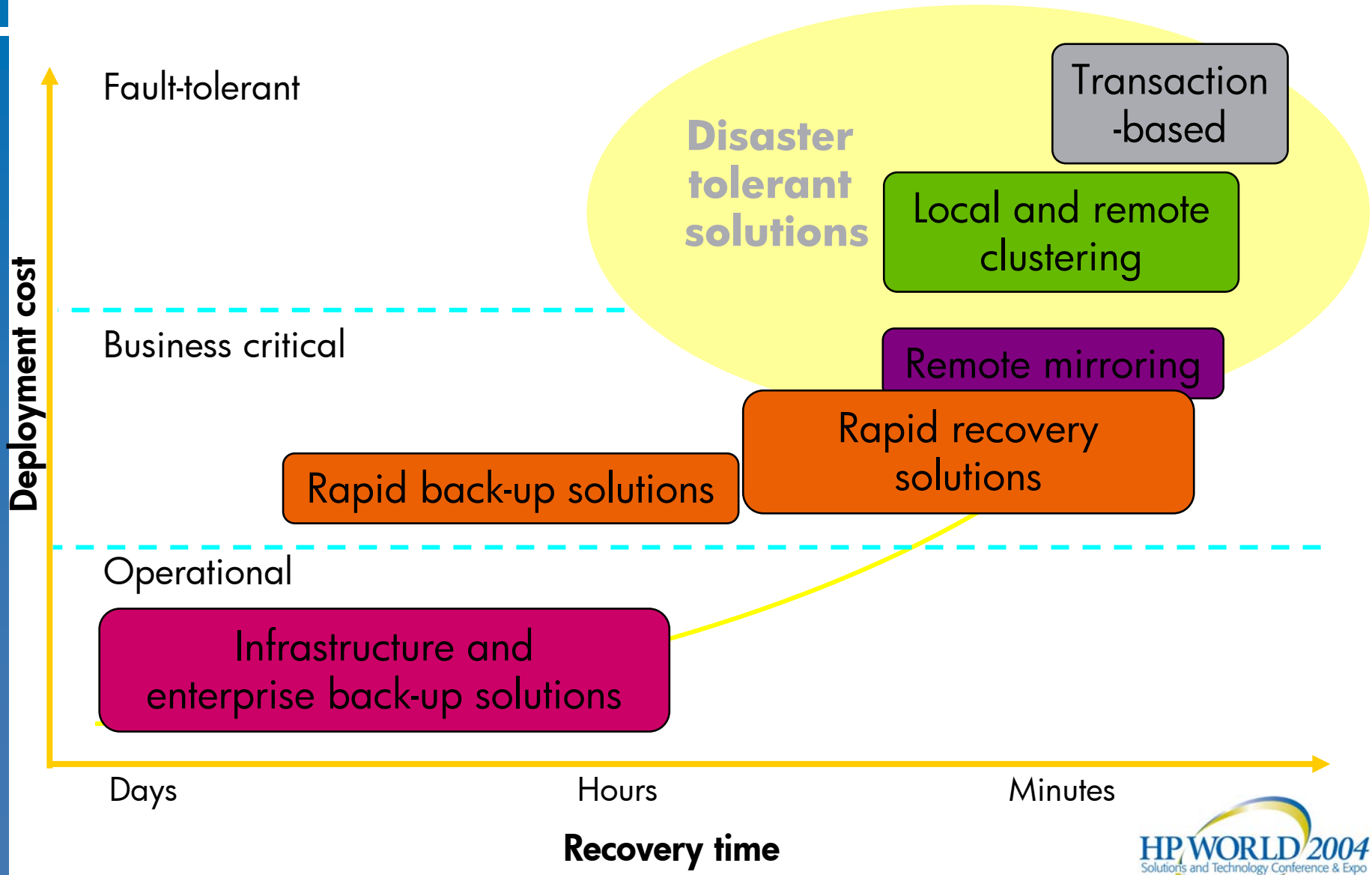
classifying recovery/continuity example

priority 1 vital	Must be available within < 1 day (24 hours) Needed for company survival Long-term financial impact Loss would have a major impact on ability to continue business Affects entire organization Severe constraints and legal liabilities	DNS Network Call Center HA systems High profile customers
priority 2 critical	Must be available within > 1 day and < 5 days Essential for company operation and to run after priority 1's Significant and necessary to maintain control of business operations Affects multiple departments Moderate financial impact	Shared hosting systems Customer support DB Provisioning
priority 3 important	Must be available within 6-7 days Not necessary for daily operation but to run as soon as the data center has capacity Loss of these applications would have some impact Minimal financial impact	Sales application Billing Payroll Shared hosting customers
priority 4 deferrable	Not needed for immediate company survival These applications are for supporting departments and can be suspended for a specified time period without significant impact because of manual backup in place Minimal to no financial impact	Program Development Training

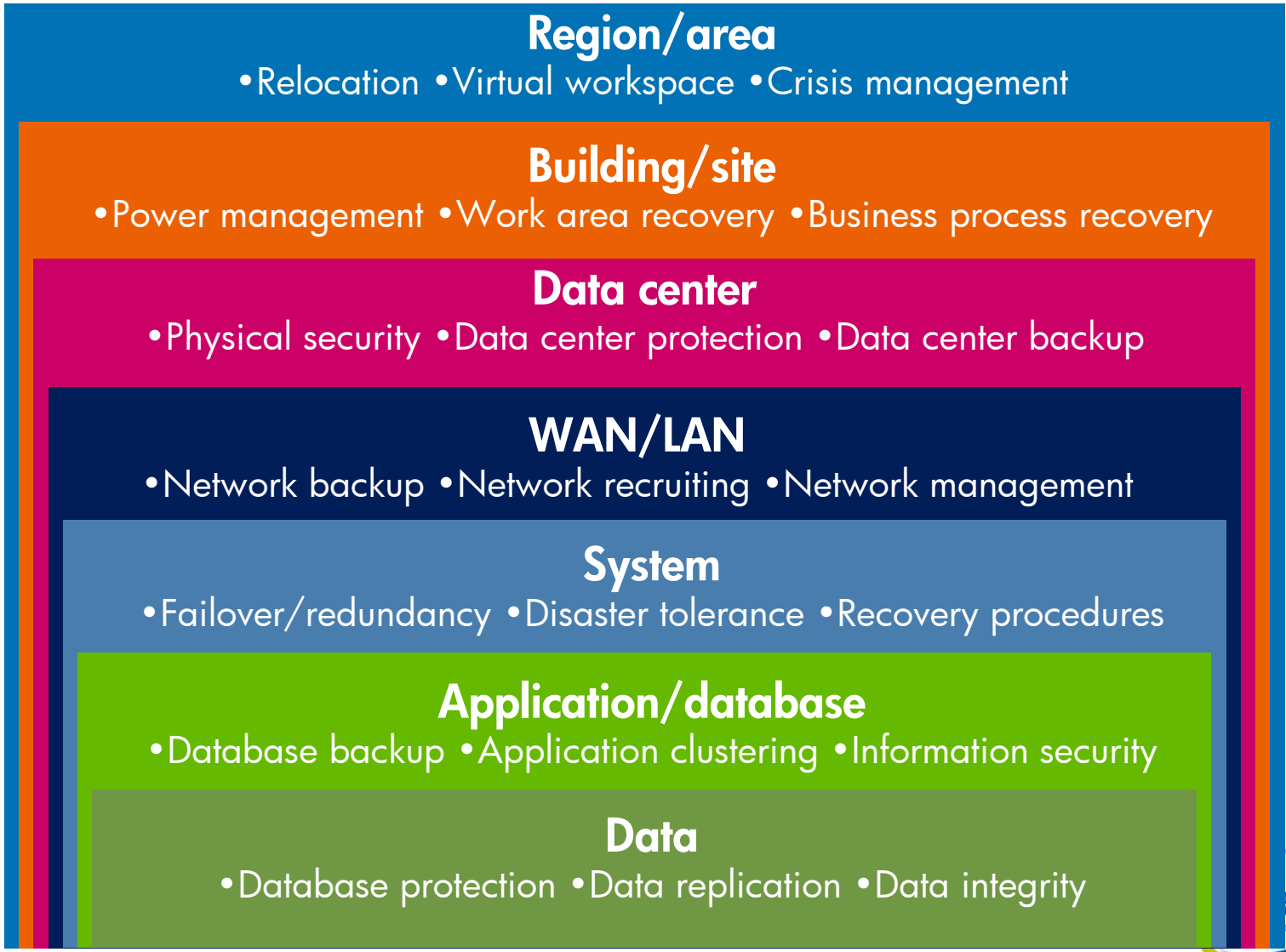
best practices: design

- ✓translate business needs into recovery and continuity strategies using timelines for recovery, continuity, and "return-to-normal"
- ✓design overall strategy for worst-case scenario
- ✓design supporting infrastructure that includes people, process, and technologies
- ✓assess existing infrastructure to meet availability and continuity requirements
- ✓design redundancy, high-availability, and replication into infrastructure

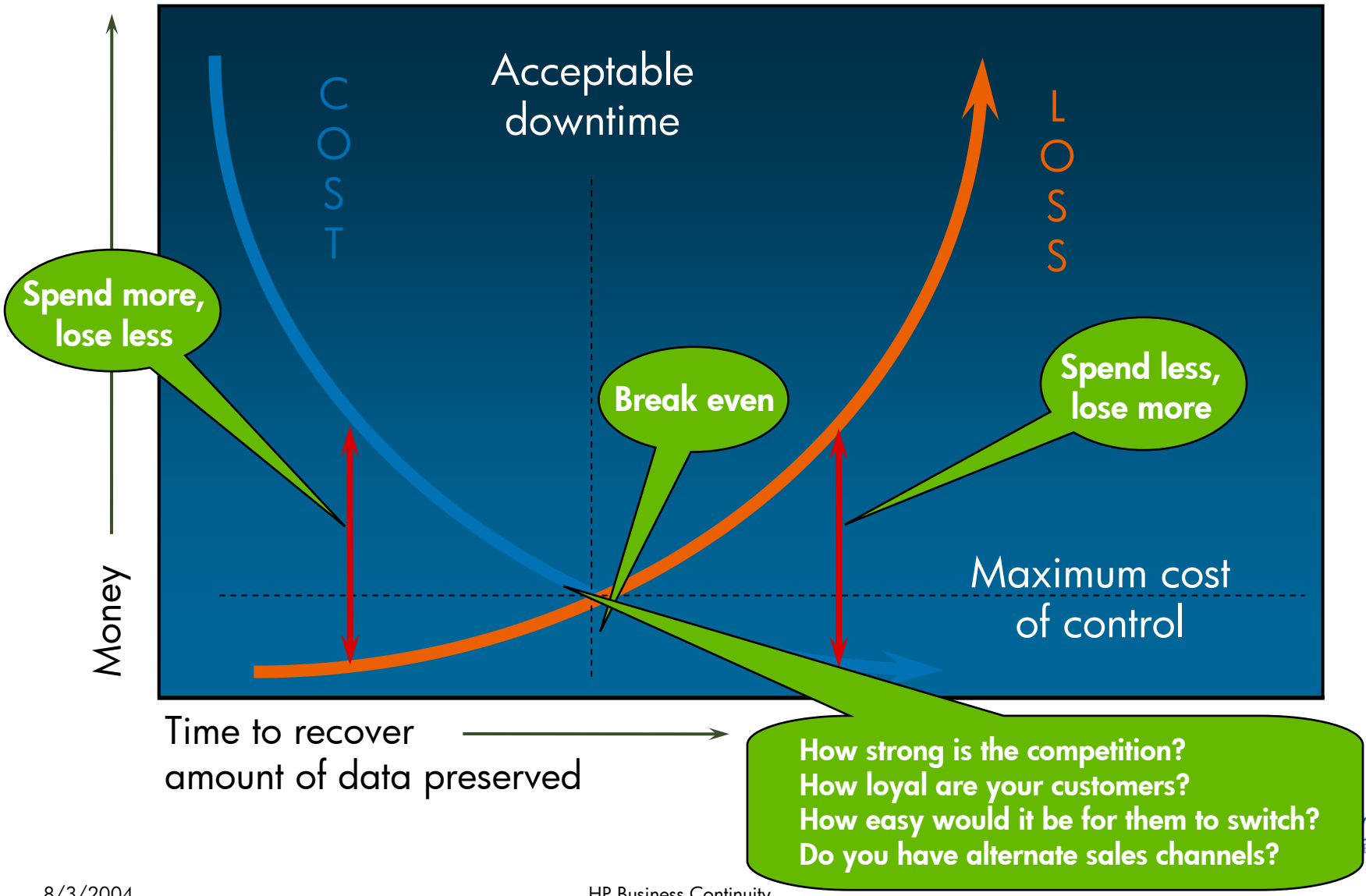
A range of recovery strategies



Business continuity: the elements at risk



Identifying your pain point



best practices: build & integrate

- identify backup locations
  - control or command center(s)
  - IT (systems/network/data)
  - work area recovery (users)
- build business continuity plan
  - structure & plan components
  - notification, escalation, & declaration processes
  - recovery/failover procedures for data, systems, network (voice/data)
  - business process recovery procedures
  - "return-to-normal" and failback procedures
  - include vendors & partner necessary to process critical business
  - process for rebuild and resumption

Lessons learned from September 11

- Loss of life and total loss of facilities
- E-mail was business critical
- Data recovery was solid, the problem was with paper
- Employee movement and transportation issues – "scale" issues
- Secondary sites for employee work areas usually unacceptable
- Long-term recovery not addressed
- Slimmed-down web sites and web sites as information exchange
- Communication issues were rampant
- Missing workflow & logistics

Meta, 2002

best practices: manage

- rehearsals
  - small scale to large scale
  - logistics to technology
  - planned & unplanned
- design rehearsal plans & schedule (include cross training)
- use outside sources as role of observer during rehearsal(s)
- post-mortems to review rehearsal results, implement feedback into BCP for changes to infrastructure & processes, identify training issues
- plan 10-15% of BC budget for rehearsals

best practices: evolve

- ensure business continuity program and plan is incorporated into the change management process
- ensure production and backup or alternate site are in sync
- implement business continuity plan review schedule and checkpoints
- on-going evaluation of deploying new technologies and processes to meet changing business needs and RTO/RPOs
- ensure on-going communication through newsletters/emails of continued efforts

Key observations

- Wide disparity in BC/DR practices across companies
- Best in class practitioners focus on "constant program improvement"
- Catch-up organizations have higher dependencies on vendors to help them solve the problem
- 50% of organizations have business interruption insurance; however, find the claims are difficult to prove
- DR/BC success is 80% people, 15% data, 5% technology

source: 2002 meta group survey, approximately 1300 clients

SARS -- business continuity management

- February 2003 – new form of pneumonia makes its way to Toronto
- HP reacted quickly after 1 suspected case is identified amongst its employees
- Split staff between two separate data centers in the Toronto area
- Identified personal contacts, e.g.., spouses, relocated to same building
- Requested staff to take laptops home daily
- Held BIA walk-throughs for each site to help be better prepared for similar future incidents (technical perspective)
- Placed alternate sites on standby in case other SARs cases identified
- Established travel restrictions between area sites from April 25th to May 15th
- Prepared emergency kits for key personnel (PC, cell/pager)

SARS -- challenges

- Gathering personal data for contractors
- Imposing travel restriction on Vendors and Customers
- Absenteeism report
- Complexity of Public Health Authority mandates – each region different
- Public Health Authority direction needed to change with respect to daily medical conditions
- Medical confidentiality must be maintained within communications plans – reducing the clarity and timeliness of communications

SARS -- lessons learned

- Defer to the experts – in this case, public healthcare authorities
- Reinforce the need for an updated crisis plan
- Create two crisis teams for such issues – one handling communications, one handling business continuity
- Timely communications are essential – speed will largely determine success or failure
- Communication with landlord
- Most Public Health Authorities operate with a traditional workforce concept & the IT workforce is very different

Northeast blackout

- Major outage (93,000 square miles, 60 million people) from 16:10 Thursday, August 14 to 21:03 Friday, August 15
- Started when a main power plant in Michigan tripped off, followed by many New York lines; Bruce Nuclear station shut down automatically after losing power
- Nature of disaster plan activation
- Declarations and plans implemented
  - Critical Services and Electronic Vaulting enables them to be operational within 8 to 24 hours
  - Recovery hardware commissioned, operating systems loaded and disk volumes configured, all within a few hours
  - Client began operations at the HP recovery center outside Philadelphia and was quickly back up and running.

Northeast blackout – challenges

- Multiple clients could have been affected and potentially their international operations:
  - HP Toronto recovery center handles 14 outsourced customers including:
    - One banking system supporting ATMs across Canada
    - SAP environments supporting manufacturing and financial processes
    - HP internal operations
- Need for multiple and back-up power sources
  - All operations seamlessly transitioned to UPS units, then to backup diesel generators
- Need for Disaster Tolerant & High Availability environment for mission-critical environments
  - Extensive use of NonStop servers and HP clustering technology provided on-site continuity for many customers
  - Example: customer seamlessly transferred New York processing to their San Francisco site using data replication and HP ContinentalClusters

Northeast blackout – lessons learned

- Spreading backup systems around geographically for security/continuity purposes needs to be done across hundreds if not thousands of miles.
- Future disasters may be just as likely to occur without any human intervention at all
- Know your recovery requirements and risks
- Ensure you have enough backup power and all critical components are connected
- Critical areas should have at least one corded, directly connected telephone.
- Do you have an alternate travel plan?
- You may not be able to rely on mobile (cellular) phones in a disaster.
- Electronic doo-dads may be nice… but only if they are working (toilets, faucets, etc.)
- Have emergency food and water for 3 days on hand.
- If you don't have the expertise to develop your own plan, hire professionals

best practices: getting started

- obtain senior management commitment throughout the company
- define scope and scenarios, not to rule out impossible, plan for worst-case scenario
- identify and classify disasters (problem, minor, major, catastrophic)
- use methodology that is flexible, agile, and easily adaptable to varying scenarios and situations
- define business continuity team structure and charter with clearly delineated roles and responsibilities, including management succession
- build business continuity into the company culture

Business continuity planning: balanced scorecard alignment

Financial

- Protect revenue by reducing impact of loss
- Reduce costs of response and recovery

Integration/operational excellence

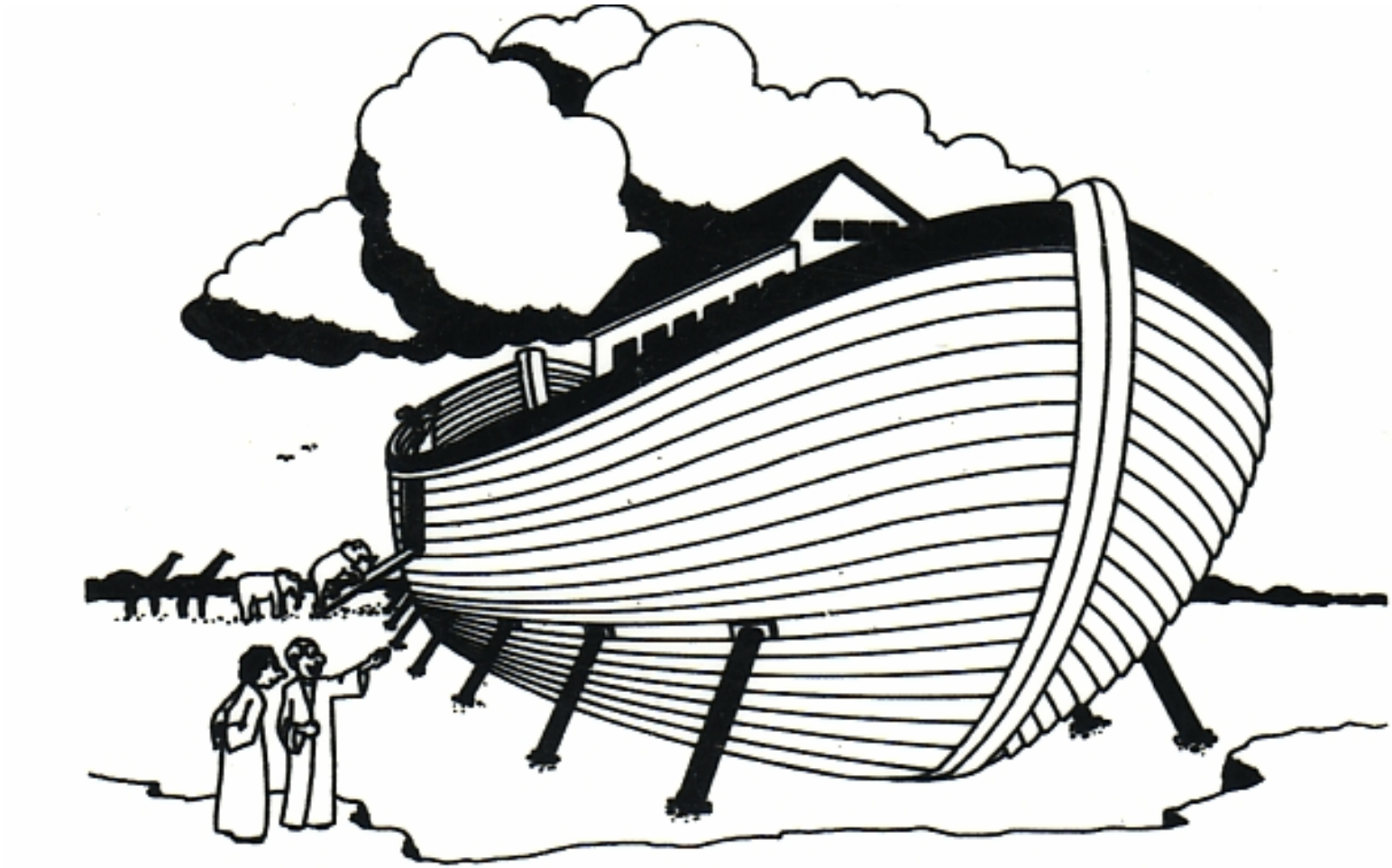
- Ensure rapid recovery
- Enable compliance with legal and regulatory requirements
- Improve operational productivity and effectiveness

Customers

- Assure ability to respond
- Reinforce confidence
- Be our own best reference

Employees

- Every employee knows that operations are safe and will continue
- Program will provide "at home" protection information



THIS IS OUR BUSINESS RECOVERY PLAN

ALL OPERATING UNITS MUST HAVE A BRP

Workshop Case Studies (handouts)

www.hp.com/hps/continuity

1-800-863-5360