The Value of Business Continuity Planning

John Zannos
Manager, Business Development
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 & terms related to Business Risk Mitigation
What is Business Continuity?

**It is...**

- A way of doing business and continuing to stay in business
- A plan to assure business processes - including suppliers and service providers - are always available to meet critical needs
- An integrated approach to link IT availability management and continuity and recovery
- An on-going effort to improve IT service levels and availability to meet the needs of the business

**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

The goal is to *achieve* business continuity, where critical business processes are operational and available to meet critical business needs
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
  - backup & recovery
  - business process recovery
  - business impact/risk management
  - continuity planning
  - security
  - disaster tolerance
  - proactive support
  - high-availability
  - IT management

- business process recovery
- business impact/risk management
- continuity planning
- security
- disaster tolerance
- proactive support
- high-availability
- IT management
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.

versus

IT Continuity Planning

A 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):**
This is the window of time from the start of an event/outrage to when the impact on the business becomes too great, causing damage to the businesses reputation and/or revenue.

**Recovery Time Objective (RTO):**
This is the window of time from a declared disaster to when the impact on the business becomes too great causing damage to the businesses reputation and/or revenue.

**Recovery Point Objective (RPO):**
This is the point in time at which your data is recovered or restored. Considered a measure of allowable data loss

**Escalation and Fix Window:**
The MTO – RTO = Escalation/fix window. This is the time from an outage to time when a disaster declare decision should be made.

**Business Impact Analysis (BIA):**
The process of analyzing all business functions and the effect that a specific disaster may have upon them. This process determines the customer MTO, Fix window, RPO & RTO.
Key Metrics for Business Continuity

Recovery Point Objective (RPO)

Recovery Time Objective (RTO)

Event

Time

Data in flight

Async.  Sync.

Provision systems

Data & application failover

Users connected
How prepared are you...
The Business Continuity Gap

• **One-third** of plans do not include recovery “sequences” for business functions.

• less than 40% of business continuity plans address resumption of operations back at the primary facility.

• less than 50% of business continuity plans deal with possible telecommunications outages.
  – 2002 META Group

• more than 40% of contingency plans in large enterprise corporate environments are NOT implementable.
  – Disaster Recovery Institute

• plans without C-level sponsorship are less likely to succeed, especially when they are left out of a corporate change management process
  -- AMR Research
Common business continuity concerns

• I have a distributed, multivendor IT environment. How do I cost effectively recover it?

• How do I ensure little or no downtime and no lost transactions?

• How do I maintain continuity in the face of my changing IT and business environment?

• How do I meet new regulations mandating business continuity?

• How do I protect my mission-critical applications and business processes?
Changes in the Market

- BC moving up in the decision-making chain
- BC moving outside of IT to include operations/functions
- “disaster” definition changing to be a combination of events
- BC plans still focused on mainly on assets (not people & processes; geographic dispersion)
- executive sponsorship and governance models
Steps to ensure success
HP Business Continuity Planning
Process Model

Analyze
- Identify and mitigate business risks and exposures
- Quantify cost of outage of key business processes (direct, indirect)
- Identify and define requirements to support critical business processes for recovery time (downtime) and recovery point (data loss)

Design
- Translate availability continuity recovery requirements and executable strategies
- Define specific options per each business process according to scenario
- Build strategies to meet recovery time objectives (RTO) and recovery point objectives (RPO)

Manage/evolve
- Rehearse the business continuity plan on a regular basis, using results to update or fine-tune the plan, as well as to identify training needs
- Use a review plan schedule with varying parties to occur on a regular basis
  - Integrate into change management process

Build/integrate
- Deploy supporting architecture to minimize downtime and achieve RTO and RPO requirements through services and technologies
- Develop overall business continuity program and plan which will tie all the pieces together, as well as outline the processes to ensure continuity for the business
How do you build enforceable IT Continuity Plans?

Have professionals that can help you:

- Understand your risks
- Determine what IT components are critical to your reputation and revenue and components that will financially effect the business in an outage
- Build recovery strategies that meet your recovery time objectives and reduce the risk of financial impact
- Write and document IT Continuity Plans
- Train staff to invoke your IT Continuity Plan
- Train staff to recover in the defined RTO window before financial impact occurs
- Manage rehearsals to ensure your plan is invoke able, stays invoke able and provide continuous training
- Maintain your plan and keep it a living document
A Range of Recovery Strategies

- **Fault-tolerant**
  - Infrastructure and enterprise back-up solutions
  - Rapid back-up solutions
  - Remote mirroring
  - Rapid recovery solutions
  - Disaster tolerant solutions

- **Transaction-based**

- **Business critical**

- **Operational**

- **Deployment cost**

- **Recovery time**
  - Days
  - Hours
  - Minutes
Critical IT Recovery Steps

It is important to understand

1. **Response:** How we respond to an event; how we escalate the event; who to escalate to; who manages the event; crisis management; declaring a disaster; disaster management team; establishing a command center.

2. **Recovery:** How we recover each of the critical IT components; how we recover the infrastructure; who recovers; which order do critical process flow.

3. **Restoration:** Access and facility process; damage assessment; restoration order and process.

4. **Resumption:** Assigning resumption teams; mapping the resumption process.

5. **Postmortem:** What did not work; what worked; what did each critical recovery time line look like.
Business continuity
The elements at risk

- **region/area**
  - relocation • virtual workspace • crisis management

- **building/site**
  - power management • work area recovery • business process recovery

- **data center**
  - physical security • data center protection • data center backup

- **WAN/LAN**
  - network backup • network recruiting • network management

- **system**
  - failover/redundancy • disaster tolerance • recovery procedures

- **application/database**
  - database backup • application clustering • information security

- **data**
  - database protection • data replication • data integrity
Financial cost of downtime is relative to who feels the pain

<table>
<thead>
<tr>
<th>Industry</th>
<th>Application</th>
<th>Average Cost per Hour of Downtime (U.S. dollars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>Brokerage operations</td>
<td>$7,840,000</td>
</tr>
<tr>
<td>Financial</td>
<td>Credit card sales</td>
<td>$3,160,000</td>
</tr>
<tr>
<td>Media</td>
<td>Pay-per-view</td>
<td>$183,000</td>
</tr>
<tr>
<td>Retail</td>
<td>Home shopping (TV)</td>
<td>$137,000</td>
</tr>
<tr>
<td>Retail</td>
<td>Catalog sales</td>
<td>$109,000</td>
</tr>
<tr>
<td>Transport</td>
<td>Airline reservations</td>
<td>$108,000</td>
</tr>
<tr>
<td>Entertainment</td>
<td>Tele-ticket sales</td>
<td>$83,000</td>
</tr>
<tr>
<td>Shipping</td>
<td>Package shipping</td>
<td>$34,000</td>
</tr>
<tr>
<td>Financial</td>
<td>ATM fees</td>
<td>$18,000</td>
</tr>
</tbody>
</table>

Source: Contingency Planning Research
Identifying your pain point

- spend more, lose less
- spend less, lose more
- break even
- acceptable downtime

- cost
- loss
- money

- time to recover
- amount of data preserved

how strong is the competition?
how loyal are your customers?
how easy would it be for them to switch?
do you have alternate sales channels?
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?
Lessons Learned
Best Practices
SARS - Business Continuity Management

- Split staff between sites
- Identified personal contacts, ie. Spouses, relocated to same building
- Requested staff to take laptops home daily
- Held BIA walk thru’s for each site (technical perspective)
- Placed alternate site’s on standby
- Assisted customers who invoked their BCP’s
- Established travel restrictions between sites from April 25th to May 15th
- Prepared emergency kits (PC, cell/pager)
SARS - Challenges

- Gathering personal data for contractors
- Imposing travel restriction on Vendors
- 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 Background

- Major outage (93,000 square miles, 60 million persons) was from 16:10 Thursday August 14 to 21:03 Friday August 15.

- It 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.
Northeast Blackout -- HP Response

• 1 HP customer called to activate disaster plan
  − Customer has a Critical Services and Electronic Vaulting agreement enabling them to be operational within 8 to 24 hours
  − Recovery hardware was commissioned, the operating systems were loaded and disk volumes were all configured and ready to go, all within a few hours.
  − The client began operations at the HP recovery center outside Philadelphia and was quickly back up and running.

• 2 more HP customers put us on notice, but never had to implement their plan
Northeast Blackout – HP response

- HP Toronto recovery center handles 14 outsourced customers including:
  - One banking system that supports ATMs across Canada
  - SAP environments supporting manufacturing and financial processes
  - HP internal operations

- All operations were seamlessly transitioned to UPS units, then to backup diesel generators when outage hit
Northeast Blackout – Onsite Continuity

• Extensive use of NonStop servers and HP clustering technology provided on-site continuity for many customers

• Example - customer with data centers in both New York and San Francisco seamlessly transferred New York processing to the San Francisco site using data replication and HP's ContinentalClusters — the most flexible of HP-UX's suite of geographically dispersed clusters.
Northeast Blackout – Lessons Learned

• Spreading backup systems around geographically for security/continuity purposes needs to be done across hundreds if not thousands of miles. Building a backup facility across the river just doesn't cut it. Companies will need to rethink what it means to create truly redundant business operations.

• While security analysts have painted a fearful picture of what would happen if terrorists combined a major attack with a well-timed and well-executed cyber-assault, a similarly nasty one-two may be just as likely to occur without any human intervention at all

• Know your recovery requirements and the risks you face.

• Ensure you have enough backup power and all critical components are connected to it.
Northeast Blackout – Lessons Learned

- Critical areas should have at least one corded, directly connected telephone.
- If your plan requires employees to travel by air to a backup site, do you have an alternate travel plan?
- You may not be able to rely on mobile (cellular) phones in a disaster. If your plan relies on them, consider changing it now.
  - Amateur radio operators can help with people and property safety. Start a club at work (HP has one)
- 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.
  - Should your company have a program to give employee discounts on bundled kits?
- If you don’t have the expertise to develop your own plan, hire professionals
Lessons Learned from September 11

- loss of life and total loss of facilities – unlike other regional disasters in that it centered on server and workplace environment (not datacenter)

- e-mail was business critical

- data recovery was solid, the problem with paper

- employee movement and transportation issues – “scale” issues

- secondary sites for employee work areas were usually unacceptable

- long-term recovery not addressed (typical contract is for 6 weeks, typical DR activation is for 2-5 days)

- slimmed-down web sites and web sites as information exchange

- communication issues (right information to the right people) were rampant

- missing workflow & logistics (fax, copiers, shipping/receiving, mail, food service, etc.)

Meta, 2002
Key Observations

• wide disparity in BC/DR practices across companies (due to vertical industry, geography, corporate culture)

• 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, and 5% technology

source: 2002 meta group survey, approximately 1300 clients
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