Business Continuity, Disaster Recovery, and Risk Analysis

Paulo Beck
Security and Business Continuity Practice Principal
Hewlett-Packard, Latin America & Caribbean Region

XXVI
Salón de Informática

La gobernabilidad de TI: Una responsabilidad y reto para los directivos de TI
Agenda

• Why Business Continuity & Availability is top of mind issue today
  – The concepts of Business Continuity
  – BC&A Terminology
  – Industry trends
  – Customer needs

• Roadmap for a Business Continuity Plan
  – Risk Analysis
  – Recovery Strategies
  – Plan Documentation
  – Continuity Management
  – Change Management Integration

• New tool to get Started
  – On-line self-assessment

• Questions and Answers
HP Market research: Business Continuity & Availability

Q05 - Which of the following business continuity/disaster recovery initiatives is your company engaged in?

<table>
<thead>
<tr>
<th>Disaster Recovery Initiative</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disaster recovery project underway</td>
<td>39%</td>
</tr>
<tr>
<td>Assessing costs and benefits</td>
<td>36%</td>
</tr>
<tr>
<td>Just completed a disaster recovery project</td>
<td>35%</td>
</tr>
<tr>
<td>Actively seeking solutions</td>
<td>26%</td>
</tr>
<tr>
<td>Planning to pursue disaster recovery within the year</td>
<td>18%</td>
</tr>
<tr>
<td>None of these</td>
<td>5%</td>
</tr>
</tbody>
</table>

- Nearly two in five (39%) of participants are currently engaged in a disaster recovery project.
- 36% are assessing costs and benefits of BC&A.
- 26% are actively seeking solutions.
Business Continuity & Availability Cycle

The business processes are supported by assets
Understanding the BC Cycle

- Natural disaster — fire, flood, adverse weather
- Man made disaster — terrorism, malicious damage
- Security breach — hacker
- Virus attack
- Internal security/fraud
- Hardware failure
- Application failure
- Network failure

• Lack of controls
What if:
- E-mail goes down for half a day
- Internet site goes down
- Call center is offline
- The ATM network, settlements, trading system crashes
- The payments/billing system fails
- Information systems are subject to a virus or denial of service attack
- Data is lost, corrupted or stolen
- Data cannot be retrieved
What is business continuity & availability?

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
Why Business Continuity & Availability is top of mind issue today?
The pressure to mitigate business & IT risk seems to be increasing…

External & business

• External threats seem more visible, frequent
• New security risks emerge each month
• Requirements grow for compliance & risk management to protect corporate reputation

Customers & service levels

• Web-based business & demanding customers require better level of IT service
• More applications & processes are becoming business-critical
• Potential to use high availability as a differentiator

Operational & technical

• 24 x 7 global operations shrink the window for back-up & downtime
• Mergers & IT consolidation put more pressure on centralised IT systems
• Dynamic business & IT environment impacts continuity and IT processes more often
Customers are asking tougher questions...

Do we really need a disaster recovery plan?

Do we have service level agreements with our users?

If the system fails, how quickly can it recover?

Am I sure that my business can keep going in a crisis or emergency?

Are we building operational excellence into our IT service?

How can we get the right levels of security & availability in our new system from day one?
What is the roadmap for a Business Continuity plan?
HP Business Continuity Consulting Services

- Integrate into change management process
- Audit/assess environment for improvements
- Service level reporting and analysis

- Ongoing monitoring, measurement, and management
- Automation of IT processes
- Test/rehearse BC&A plan regularly

- Identify & mitigate business and operational risks.
- Quantify cost of outage of key business processes (direct & indirect)
- Define availability and objectives for each business process

- Evaluate strategy & technology alternatives
- Architect solution to meet objectives (including detailed design of infrastructure and processes)

- Develop overall BC&A plan to ensure continuity for the business
- Implement and integrate infrastructure and processes.
- Train staff.
1. Risk Analysis
HP's approach encompasses a hierarchy of elements at risk

<table>
<thead>
<tr>
<th>IT service management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service continuity — Availability management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Region/area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crisis management — Disaster tolerance — Virtual workspace</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Building/site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power management — Work area recovery — Hot site</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Center/physical environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical security — Data center protection — Data center backup</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WAN/LAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network backup — Network redundancy — Network management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application/database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database protection &amp; backup — Application availability — Data security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware and software — Failover/redundancy — Recovery &amp; repair procedures</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data/storage/SAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database protection — Data replication — Data integrity &amp; availability</td>
</tr>
</tbody>
</table>
Customers need to identify business & IT risks...

- natural disaster - fire, flood, adverse weather
- man made disaster - terrorism, malicious damage
- security breach - hacker
- denial of service attack
- virus attack
- internal security/fraud
- Compliance risk
- application failure
- power/ network failure
- software failure
- hardware failure
- planned downtime

Impact vs. Frequency Matrix:
- High Impact:
  - natural disaster
  - man made disaster
  - security breach
  - denial of service attack
  - virus attack
  - internal security/fraud
- Low Impact:
  - Compliance risk
  - application failure
  - power/ network failure
  - software failure
  - hardware failure
  - planned downtime

- Low Frequency:
  - natural disaster
  - man made disaster
  - security breach
  - denial of service attack
  - virus attack
  - internal security/fraud
- High Frequency:
  - Compliance risk
  - application failure
  - power/ network failure
  - software failure
  - hardware failure
  - planned downtime
.. they should understand the potential causes of downtime...

Causes of unplanned downtime

- Software System Failure: 27%
- Hardware System Failure: 23%
- Human Error: 18%
- Network Transmission Failure: 17%
- Environmental Factors (Natural Disaster): 8%
- Uncertain: 7%

Source: CPR, a division of Eagle Rock Alliance, Ltd., West Orange, NJ.
.. and consider the cost of outages in their own organisation

- Downtime costs can be very high
  - The cost of downtime depends on the industry and the application affected

- For Internet based businesses, IT downtime is business downtime

- Some analysts suggest that up to 10% business costs are associated with IT downtime and outages
Businesses are asking for fast answers...

<table>
<thead>
<tr>
<th>Time Frame</th>
<th>Duration</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 minutes</td>
<td>5 seconds</td>
<td>Market analysis</td>
</tr>
<tr>
<td>20 minutes</td>
<td>30 seconds</td>
<td>Air ticket</td>
</tr>
<tr>
<td>8 hours</td>
<td>10 seconds</td>
<td>Call Center calling</td>
</tr>
<tr>
<td>1 day</td>
<td>5 minutes</td>
<td>Financial update</td>
</tr>
<tr>
<td>1 day</td>
<td>15 minutes</td>
<td>Supply Chain update</td>
</tr>
<tr>
<td>3 days</td>
<td>30 seconds</td>
<td>Fax / e-mail</td>
</tr>
<tr>
<td>3 days</td>
<td>45 seconds</td>
<td>Document transfer</td>
</tr>
<tr>
<td>3 days</td>
<td>1 hour</td>
<td>Phone activation</td>
</tr>
<tr>
<td>1 mês</td>
<td>1 hour</td>
<td>DW recovery</td>
</tr>
<tr>
<td>5 days</td>
<td>1 day</td>
<td>POS initiation</td>
</tr>
<tr>
<td>6 weeks</td>
<td>24 hours</td>
<td>PC instalation</td>
</tr>
</tbody>
</table>

10^7 10^6 10^5 10^4 1,000 100 10 1 seconds
What is the impact of these risks?

**Revenue:**
Direct loss, compensatory payment, lost future revenues, billing losses and investment losses

**Productivity:**
Number employee x impacted x hours out x burdened hours = ?

**Damaged reputation:**
Customers, competitors gain advantage, suppliers, financial markets, business partners

**Financial performance:**
Revenue recognition, cash flow, credit rating, stock price, regulatory fines

Indirect impact of downtime can be far more severe and unpredictable
Risk Analysis - Identifying your Customer’s Pain points

- Maximum cost of control
- Acceptable downtime
- Break Even
- More investment, Low Risks
- Low investment, High Risks

What is the competitor's strengths?
What is the customer's loyalty?
Can they easily switch to another provider?
Do we have alternate commercial channels?
Risk Analysis Activities for a Business Continuity centric

- **BIA** Business Impact Analysis
  - Classify the assets vulnerability based on an assessment that identify all over threats probability and assets exposition.

- **AVA** Assets Vulnerab. Assessment
  - Security and BC&DR Workshop to understand the controls effectiveness, urgency and risk of best practices.

- **DCV** IT Downtime Cost Valuation
  - Evaluate the financial impact of an IT stoppage and downtime to define the best cost-effective solution and strategy.

- **Gap Analysis for BCP**
  - Business process classification to determine de criticity in terms of impacts on the business when assets fail because a threats became a vulnerability in the infrastructure.
Gap Analysis

• Why I need the service?
  – To compare the lack of control versus effectiveness
  – To understand the risks and the best practices needed

• What is the focus area?
  – BCP/DRP best practices and controls from DRII and BCI
  – Security best practices and controls from ISO and BS7799

• Which are the deliverables?
  – Radar graphics with control effectiveness, urgency, and risk
  – Action plan w/ short, medium, and large term vision
Assets Vulnerability Assessment

• Why I need this service?
  – To classify assets by vulnerability, based on assessments that identify probabilities of threats and assets exposition

• What is the focus area?
  – Information Technologies assets, datacenter or a specific infrastructure that is supporting critical process or business requirements

• Which are the deliverables?
  – Assets taxonomy
Business Impact Analysis

• Why I need this service?
  – To classify the business process and its criticity in terms of financial and operational impacts when assets fail because a threat became a vulnerability in the infrastructure.
  – To determine the conformity and timeframe that assets need to be recovered in accordancy w/business process requirements to assure business continuity.

• What is the focus area?
  – Critical business process

• Which are the deliverables?
  – Business process taxonomy
  – Recovery time and point objective (RTO and RPO)
  – Financial and operational business impacts
Downtime cost valuation

• Why I need this service?
  – To Evaluate the financial impact of an IT stoppage and downtime
  – To define the best cost-effective solution and strategy.

• What is the focus area?
  – Most critical business process

• Which are the deliverables?
  – Financial business impacts
2. Recovery Strategies design
Business Continuity Metrics

- **Recovery Point Objective (RPO)**
  - Point in time to which applications data must be recovered to resume business transactions

- **Recovery Time Objective (RTO)**
  - Maximum elapsed time required to complete recovery of application data
  - Business needs drive the technology choice
Recovery Strategy Activities for a Business Continuity centric

RSS Recovery Strategy Selection

Design and architecture of ideal solutions and strategies that need to be implemented to provide a high-availability environment for assets and business processes (storage, mirroring, alternate site).

Alternate Site, Storage, Servers, Extended Cluster, Mirroring, Mission-critical services, installations & configurations...

Disaster Recovery Center

High-Availability Recovery Services

Disaster Tolerant
Q07 – What are the top three technologies you are using or plan to use in a disaster recovery/business continuity project?

- Almost three-quarters (73%) of participants are currently using data replication or mirroring.
  - Other frequently-selected technologies are 3rd party recovery centers (44%) and virtualization technologies (30%).
- Large businesses are more likely to be engaged in clustering (27%, compared to 14% midsize).
How Many Data Centers is Enough?

- One (per major geography) with 3rd-party DR (72-hour recovery)
  - No single point of failure within data center (hardened)
  - Cost base is $x$
  - Over 50% of enterprises through 2006 will find one adequate

- Two data centers (per geography)
  - 8-hour recovery with critical data replicated (warm)
    - 3x cost
  - Zero outage, both centers hot
    - 4x-5x cost

- Through 2006, 40% of enterprises will follow a two-data-center scenario

Equilibrium Required

Availability and continuity requirements must be defined by business leaders and evaluated on cost vs. business risk
3. Plan Documentation
Plan Documentation Activities for a Business Continuity centric

Description of emergency procedures to assure that people and external agents will be activated in case of a crisis or disaster.

Description of crisis management procedures to assure that each threat will be handled in a crisis or disaster environment.

Description of contingency procedures to assure that the business processes will run in case of a crisis or disaster.

Description of assets recovery procedures to assure a high-availability environment, considering RTO and RPO.

BCP & DRP

Build/Integrate

3

PLAN DOCUMENTATION Emergence Response Plan

PLAN DOCUMENTATION Crisis Management Plan

PLAN DOCUMENTATION Business Continuity Plan

PLAN DOCUMENTATION Disaster Recovery Plan
4. Continuity Management
Rehearsal and Ongoing Activities for a Business Continuity centric

Ongoing services to quality and control assurance of operational procedures.

Training and communication plan to assure the usability of procedures by the personal users and managers.

Test and simulations programmes to assure quality of operational procedures (people, process and technology).

Crisis and Contingency procedures to assure effectiveness of operational procedures (people & process).

ONGOING Maintenance Plan

TRAINING
Training & Communication Plan

TEST & UPDATE
Tests, Simulations and Updating program

CONTINGENCY OFFICE
Crisis Management Center and Procedures
5. Change Management activities
Change Management Activities for a Business Continuity centric

- Audit/assess environment for improvements.
- Integrate into change management process.

AUDIT
Change Management and Quality Assurance

CHANGE MANAGEMENT
Change Management and Quality Assurance
HP Business Continuity Services offerings

**Process**
- “Analyze” Risk Analysis
- “Design” Recovery Strategies
- “Build/Integrate” Documentation Plan
- “Evolve” On-Going Activities
- “Manage” Rehearsal Activities

**Solutions**
- disaster tolerant
  - recovery objective 0 to 8 hours
- business recovery
  - recovery objective 8 to 72 hours
  - recovery objective 72+ hours
- backup/recovery
  - metrics

“Build/Integrate”
“Design”
“Evolve”
“Manage”
“Analyze”
Americas Recovery Centers

Data Center & Office Recovery Centers

- King-of-Prussia, PA
- Alpharetta, GA
- Colorado Springs, CO
- Costa Rica
- Aguadilla Puerto Rico
- Sao Paulo, Brazil (DC)
- Buenos Aires, Argentina
- Monterrey, Mexico
Business Continuity
External References
New tool to get started: On-line Self Assessment

A quick assessment allowing customers to review their overall business continuity and availability readiness

Easy to complete. Takes 10 to 15 minutes

You get a written report identifying areas for further investigation
Your BC&A Recourses

- Business Continuity and Availability Self Assessment
  - [www.hp.com/go/continuityandavailability](http://www.hp.com/go/continuityandavailability)

- Consulting Services – HP Colombia
  - [oscar.rodriguez@hp.com](mailto:oscar.rodriguez@hp.com)

- Latin America Security and BC Practice Principal
  - [paulo.beck@hp.com](mailto:paulo.beck@hp.com)
XXVI Salón de Informática