Business Continuity Management & Disaster Recovery - The Symantec Perspective
Symantec and Virtualization

- Storage Virtualization
- Server Virtualization
- Endpoint Virtualization

- Storage & Server Mgmt
- Data Protection
- Disaster Recovery
- Security & Compliance
Secure & Manage your information-driven world

Secure

- ERP/CRM
- eMail and Collaboration

Information

Manage

- Custom Apps
- Clients
The Next Phase: Standardized Infrastructure for Physical/Virtual

Physical Environment

Virtual Environment

Storage & Server Mgmt

Data Protection

Disaster Recovery

Security & Compliance
World Events Change Business Continuity Landscape

Disaster Recovery
RTO = 3 Days; Scenarios Limited

Business Recovery
for critical work processes

Y2K and BPR
RTO = < 24 hours
+ Contingency Planning

Internet and BPR
RTO/RPO ~ 1 hr
+ B-E, B-B, B-C

Aftermath of Sept. 11
Realtime RTO/RPO
+ Threat Scenarios

Business Continuity Management
+ Automation

2000
2002
2005
2007

1990
1995

Business Continuity
Proactive Failover
+ Security Scenarios
Ongoing Challenges for Achieving Business Continuity

- Interruptions to routine processes
- Impact on employee productivity and customer relationships
- Ensuring consistent process across data and applications.
- Meeting recovery point and recovery time objectives
## Elements of Business Continuity

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disaster Recovery</td>
<td>Recover mission-critical technology and applications at an alternate site.</td>
</tr>
<tr>
<td>Business Recovery</td>
<td>Recover the business process; workspace recovery.</td>
</tr>
<tr>
<td>Contingency Planning</td>
<td>Developing procedures and arrangements in advance that will support recovery</td>
</tr>
</tbody>
</table>
Business Continuity From Symantec: Getting There

1) Begin with a Business Continuity Management assessment
2) Choose appropriate architecture and accompanying configuration (Technology Independence)
3) Leverage best practices
4) Test, evaluate and monitor the BCP
Symantec Capabilities Map to Business Continuity Evolution

Backups, establishing RTO, RPO

Local mirroring, snapshots

Local clustering

Remote replication, clustering

Availability testing, systems optimization

Patch, threat management

Policy automation

<table>
<thead>
<tr>
<th>Business Continuity</th>
<th>Prevention: Protect Against and Prevent Data Loss and Downtime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Avoid outages via proactively monitoring threats and patch management policies</td>
</tr>
<tr>
<td></td>
<td>Remediation: Fix the Problem</td>
</tr>
<tr>
<td></td>
<td>Identify systems to patch, points of attack, application failures, and data loss</td>
</tr>
<tr>
<td></td>
<td>Recovery: Reach RTOs/RPOs</td>
</tr>
<tr>
<td></td>
<td>Restore data, application services to meet business recovery time objectives (RTO), recovery point objectives (RPO)</td>
</tr>
</tbody>
</table>
Business Continuity from Symantec Spans from Prevention to Remediation to Recovery

1. Prevention - Outside
   - Symantec DeepSight Threat Mgmt, Alert Services
   - Symantec Managed Security Services
   - Symantec Business Continuity Mgmt Service
   - Symantec DLP

2. Prevention - Inside
   - Symantec End Pt Protection
   - Symantec Mail Security
   - Symantec DLP

3. Prevention - Inside
   - Symantec NetBackup (Backup Exec)
   - Veritas Storage Foundation
   - Veritas Volume Replicator
   - Veritas Cluster Server
   - Symantec LiveState Recovery

Reports on attacks and outages; service levels met; RTO/RPOs achieved

1. Prevention - Outside

2. Prevention - Inside

3. Prevention - Inside

4. Remediation
   - Symantec CCS
   - Symantec Incident Manager
   - RTO/RPO steps
   - Altiris

5. Recovery
   - Symantec LiveState Client Management Suite
   - Altiris
Thank You!