Business Continuity and Disaster Recovery Planning from an Information Technology Perspective

Presenter: David Bird, Director of Sales, Business Technology Consultant
phone: 215–672–7100
e-mail: dbird@quatro.com
Table of Contents

- Introduction
- Statistics
- Recent Events
- What should we be thinking about from an IT perspective?
- Getting Started
- Key Metrics
- Best Practices
Introduction

Why should you care about this presentation?
- Increased dependence for businesses on IT;
- Reliance on business-critical information;
- Importance of protecting irreplaceable data;
- Most companies relying on their computer systems as critical infrastructure in their business;
- Most companies are aware that they need to backup their data to limit data loss and to aid data recovery;
- Most companies do not have a disaster recovery plan;
Introduction

- Why should you care about this presentation?
Introduction

- The “goal” of this presentation...
  - Is to create awareness on the basics on what you need to know about Business Continuity and Disaster Recovery Planning;
  - Learn about some proven, affordable strategies for your company;
Statistics

- Most large companies spend between 2% and 4% of their IT budget on disaster recovery planning; (Gartner Group)
- Of companies that had a major loss of computerized data without a disaster recovery plan:
  - 43% never reopen;
  - 51% close within two years;
  - only 6% will survive long-term;
Statistics

- Fires permanently close 44% of the business affected;
- The 1993 World Trade Center bombing, 150 businesses out of 350 affected failed to survive the event;
- The firms affected by the Sept. 11 attacks with well-developed and tested BCP manuals were back in business within days;
Recent Events (catastrophic occurrences)

- 9–11
- Hurricane Katrina & Wilma
- Fires in Southern California
- Tornadoes in the mid-west
- For more information:
http://www.fema.gov/index.shtm
Recent Events (human driven)

- SPAM and Virus attacks
- Cyber attacks
- Decentralized Data
- Power Outages
- Equipment Failures
- Employee Negligence
- Social Engineering
From an IT perspective, what should we be thinking about?

- What state would my business be in if we experienced one of these events?
- How long would it take for me to recover?
- Define all of the efforts needed to get us back in operation?
- How much revenue would we lose if we were “down and out” for 24, 48, 72 hours?
- How safe are my companies “crown jewels”?
From an IT perspective, what should we be thinking about?

- **Hardware Failures**
  - Storage Equipment, Servers, Firewalls, Switches, Desktops, Laptops, PDA’s, Printers, Copiers, Fax, etc.

- **Application Failures**
  - Web base, Messaging, Database, etc.

- **Telecommunications Failures**
  - Voice (land and wireless) and Data
Getting Started!

- Define some important Terms & Metrics
  - Business Continuity
  - Disaster Recovery
  - Key Business Processes
  - Business Critical Systems and Data
  - Recovery Point Objective (RPO)
  - Recovery Time Objective (RTO)
Term: Business Continuity

- Defined as:
  - A interdisciplinary concept used to create and validate a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical function(s) within a predetermined time after a disaster or extended disruption.
Term: Disaster Recovery

Defined as:
- The process, policies and procedures of restoring operations critical to the resumption of business, including regaining access to data (records, hardware, software, etc.), communications (incoming, outgoing, toll-free, fax, etc.), workspace, and other business processes after a natural or human induced disaster;
Key Metrics

- The Key Business Processes for your business...
  - Defined as is the collection of your businesses operations from which you fulfill your customer’s (internal or external) needs.
    - Customer Order Process
    - Purchasing
    - Manufacturing
    - Payroll
Key Metrics

- Business Critical Systems and Data
  - The Systems
    - IT infrastructure “the gear”
    - Operating Systems
  - The Data
    - Email
    - CRM
    - ERP
    - File Servers
    - Website
    - Phone System
Key Metrics

- Recovery Point Objective (RPO)
  - Defined as the amount of data lost measured in time.
  - Example: If the last available good copy of data upon an outage was from 24 hours ago, then the RPO would be 24 hours.
Key Metrics

- Recovery Time Objective (RTO)
  - Defined as the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.
Business Continuity Planning Lifecycle
Analysis Phase...

- Define the DR Team
- Rank your Key Business Processes
- Initiate the Planning Process
  - Impact Analysis
  - Threat Analysis
  - Recovery Requirements (business & technical)
- Compile your Business Continuity Manual
Analysis Phase...

- Business Continuity Manual
  - May be simply a printed manual stored safely away from the primary work location containing:
  - The names, addresses, and phone numbers for crisis management staff;
  - General staff members;
  - Clients and vendors;
  - Insurance contracts;
  - The location of the offsite data backup storage media;
  - Data/Systems Recovery Process
Analysis Phase...

- Business Continuity Manual
  - Include recovery requirements
    - Number and types of workstations
    - Primary and secondary locations
    - Key individuals involved in a recovery effort
    - Key applications and date
    - Maximum time allowed for an outage
    - Peripheral requirements like computers, printers, copiers, faxes, etc.
Solutions Design Phase...

- Your goal is to identify the most cost effective disaster recovery solutions based on RPO and RTO based on your companies risk tolerance levels.
Solutions Design Phase...

- Important ranking of key business applications and processes:
  - E-commerce;
  - E-mail based communications;
  - Production Processes;
  - IT Services;
  - Finance;
  - Sales and Marketing;
  - Customer Service;
  - Accounting & Reporting;
Implementation Phase…

- Complete Assessment of your IT infrastructure;
- Review the Findings Report (Health Check);
- Make the necessary improvements;
- Document the new environment;
Testing and Organizational Acceptance Phase

- Test the plan in its entirety or parts
  - Power Outages
  - Hardware Failures
  - Telecommunications Outages
  - Applications Test
  - Business Process Test
Maintenance Phase...

- Confirm the information in the manual is accurate after your testing;
- Roll out the BCP with your staff and conduct some basic training;
- Continue to test and verify the readiness of your IT solutions;
- Review the BCP on an annual basis;
Important to note…

- Firms should ensure that their BCP manual is realistic and easy to use during a crisis;
- The BCP sits alongside crisis management and disaster recovery planning and is a part of an organization's overall risk management;
Best Practices to avoid hardware failures...

- Implement a remote Monitoring and Management of your IT Infrastructure
  - Comprehensive monitoring of your equipment: Storage, Servers, Switches, Firewalls, Computers, etc.;
  - Proactive Management to prevent Cyber Attacks;
Best Practices in the event of a hardware failure…

- Implement a Back-up and Data Restore Process
  - Utilize a centralized, automated back-up for your company PC’s, files, applications, and data base servers, storage units;
Best Practices in the event of a power outage…

- Due to power outages…
  - Implement a battery back up solution and surge protection strategy;
  - Consider a diesel generator for your data center of facility;
Best practices to avoid application failures...

- E-mail Application Defense
  - Spam and viruses filtering before they enter your network;
  - Implement a Hosted E-mail service with a provider that utilizes a secure, fully redundant data center;
  - Implement a replica of your email systems in a data center;
  - Keep your desktops, laptops and PDA’s secure from viruses and theft;
Best practices to avoid application failures…

- Website Protection
  - Secure your website in a secure, fully redundant data center;
  - Implement geographic redundancy for your website;
  - Make sure you have a back-up of your website;
Best Practices to Communications Failures…

- Voice and Data Service Protection
  - Implement a phone system redundancy;
  - Hosted VOIP
  - Don’t rely on a single Internet or Voice provider;
  - Implement redundant connectivity;
  - Move the critical systems to a hosted fully redundant environment;
Who does this Stuff?

- Your IT Department
- Enterprise Account DR Providers
  - Sungard
  - Hewlett-Packard
- Regional Provider specializing in the SMB Market
  - Make sure they have vast industry experience:
    - Disaster Recovery & Business Continuity Planning
    - Data Center and Hosting Solutions
    - Enterprise Storage Solutions
Quatro’s Approach

- Business Continuity Consulting, Planning and Implementation
  - Readiness Review
  - Risk Assessment
  - Business Impact Analysis
  - Recovery Strategy Development
  - Business Continuity Plan (IT)
  - Rehearsal & Test Support
- Affordable Availability Services
  - Hosting
  - Co–Location
  - Server and Application Image
  - Remote Back Up and Replication
  - Data Storage
  - Hot Site
  - Security (SPAM & Virus)
How do I contact you?

- David Bird
  - Phone 215–672–7100 ext. 288
  - Email dbird@quatro.com
  - www.quatro.com
Thanks!