

Business Continuity and Disaster Recovery

Keith R. Anderson
Commercial Sales Engineer
TWC Business Class

September 28th, 2011



Agenda

- Changing Business Environments
- Wake Up Calls
- Types of Disaster
 - Man Made
 - Natural Disasters
- What is Business Continuity
- Business Continuity Planning
 - Network Security
 - Data Security



Changing Business Environment

- Electronically Stored Information Assets
- Customer Relationship Management (CRM)
- Customer Service
- Financial Records
- Point of Sale
- Accounts Receivable
- Employee Records/HR
 - Employee Access to the Internet
- Regulatory Concerns
 - HIPAA / SOX / Graham Leach Bliley / ???



The Wake Up Calls -Real World Data Loss

- Hurricane Andrew 1992 (Pre Internet)
- Hurricane Katrina 2005
 - Insurance replaces buildings, office furniture and computers, but what about my Data??
 - **\$41.9 Billion** in Business Losses
- Man Made Disasters
Hackers, Viruses, Malicious Employees



The Experts All Agree:

“A Company that experiences a computer outage lasting more than 10 days will never fully recover financially. 50 percent will be out of business within five years.”

An estimated 25 percent of businesses do not reopen following a major disaster

70 percent of small firms that experience a major data loss go out of business within a year.

- Of companies experiencing catastrophic data loss:
 - • 43% of companies never reopened
 - • 51% of companies closed within 2 years
 - • 80% of companies that do not recover from a disaster within one month are likely to go out of business.
- **75% of companies without business continuity plans fail within three years of a disaster**

Source: U.S. Small Business Administration



Develop a Plan - Initial Questions to Ask

1. **Offsite:** How do you access data if the building is inaccessible?
2. Is Information **security** important to you? Do you **encrypt** your data?
 - a) If you lose a tape/drive with your client data, does that impact your business?
 - b) Are you regulated?
3. How do you **verify** your backups?
 - a) How do you know if the data is on the backup unit?
 - b) How do you protect against a virus being backed up?
4. Do you have a **retention** policy? How far back do you backups go?
 - a) How do you protect against a deleted file that is unnoticed?
5. **Who** administers backups and controls recoveries? How much time is spent?
 - a) Do you have to rely on an IT consultant?
 - b) How do you manage multiple sites?
6. How much **downtime** can you afford? Recovery time objective?
7. Are tapes your **long term strategy**?
8. **What is the financial impact of a data loss?**



Business Continuity Planning- Network Security

- Network and Internet Questions
- What are my liabilities if my employees misuse my Internet ?
- Do I have a Firewall?
- Hardware vs. Software
 - ♦ Is my e-mail Filtered?
 - ♦ What are my options for Anti-Virus?
 - Resource Servers
 - Software

What do I need to protect?



After you have asked the Questions

- Write down the answers.
- Brief Key players
- How detailed ?
 - How important is it that you stay in business?
 - Examine all your options, which are:



Options.....

- Software: Anti Virus, Clients
- Hardware: Firewalls
 - Web filtering
- Storage Facility-other locations(internal)
 - Off Site providers
- IT knowledge
- Human Intervention
- LUCK
- Cloud Services



Nothing



Question and Answer

- What do you do now?

