CyrusOne

New Trends of Business Continuity

Dan Vazquez
Vice President, Technology

September 2004

CyrusOne

State of Business Continuance

- No tolerance for downtime
  - The evolution of business requirements
  - ERP systems, supply chain management, CRM, e-business
  - Continued access to information is critical
- With pushing information closer to the customer comes some risk; customers now may know you have issues before you do
- Response times becomes more critical
- Managing system resources becomes more critical

State of Business Continuance

- What is the greater risk to companies today (Natural Disaster or Worms/exploits)?

- The goal; continuous availability of networks and systems
- The means
  - Proper engineering, security, and failover
  - Not retrofitting a disaster recovery plan
  - Designing with business continuance in mind
  - Engineering a solution; not a bandage

CyrusOne

State of Business Continuance

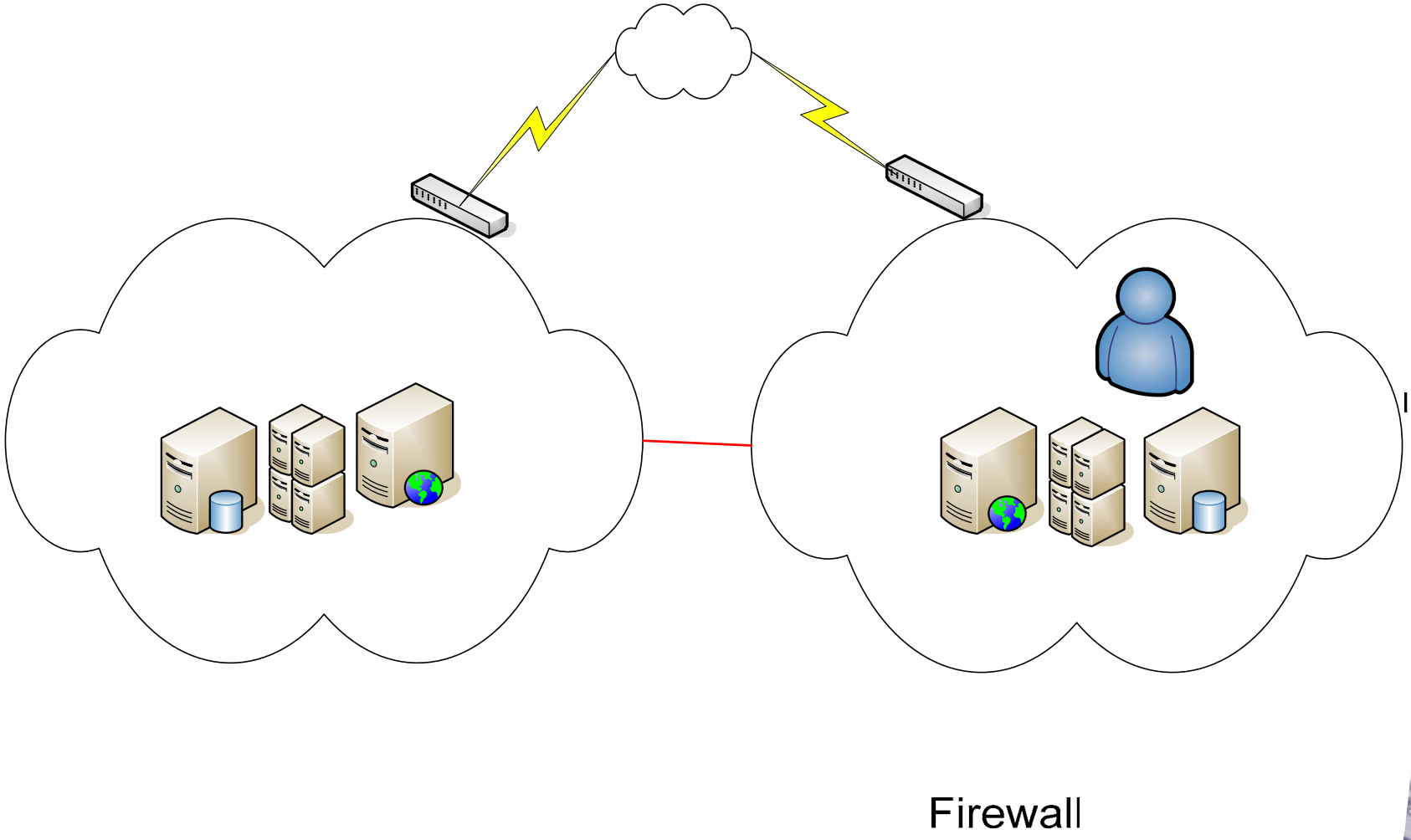
Trend Micro findings, (16 Jan 04):

- It is estimated that PC Viruses cost businesses approximately $55 Billion in damages in 2003

TruSecure / ICSA Labs (29 August 03):

- Survey of over 882 respondents on MS Blaster worm impact
- Remediation cost $475,000 per company *(median average - including hard, soft and productivity costs)* with larger node-count companies reporting losses up to $4,228,000
- Company networks entered most often through infected laptops, then through VPNs, and finally through mis-configured firewalls or routers

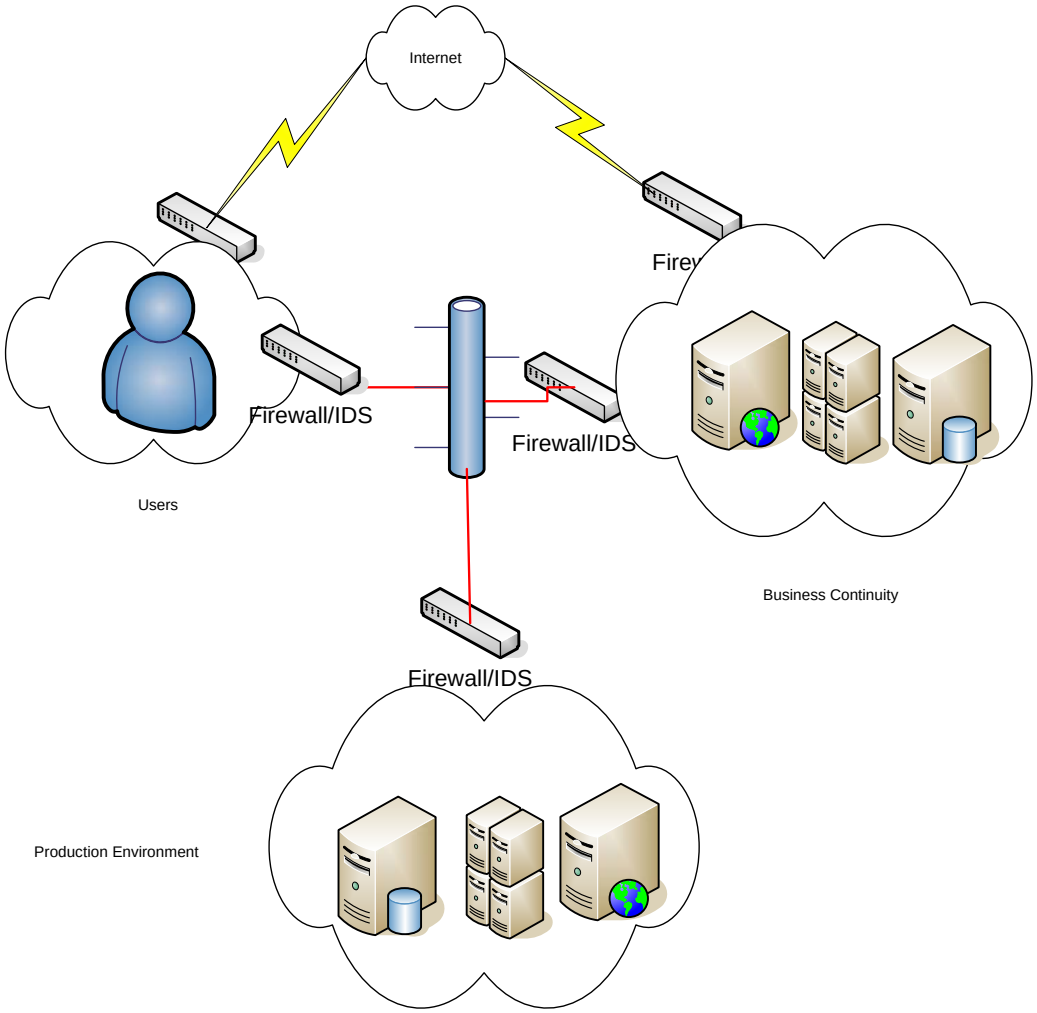
State of Business Continuance



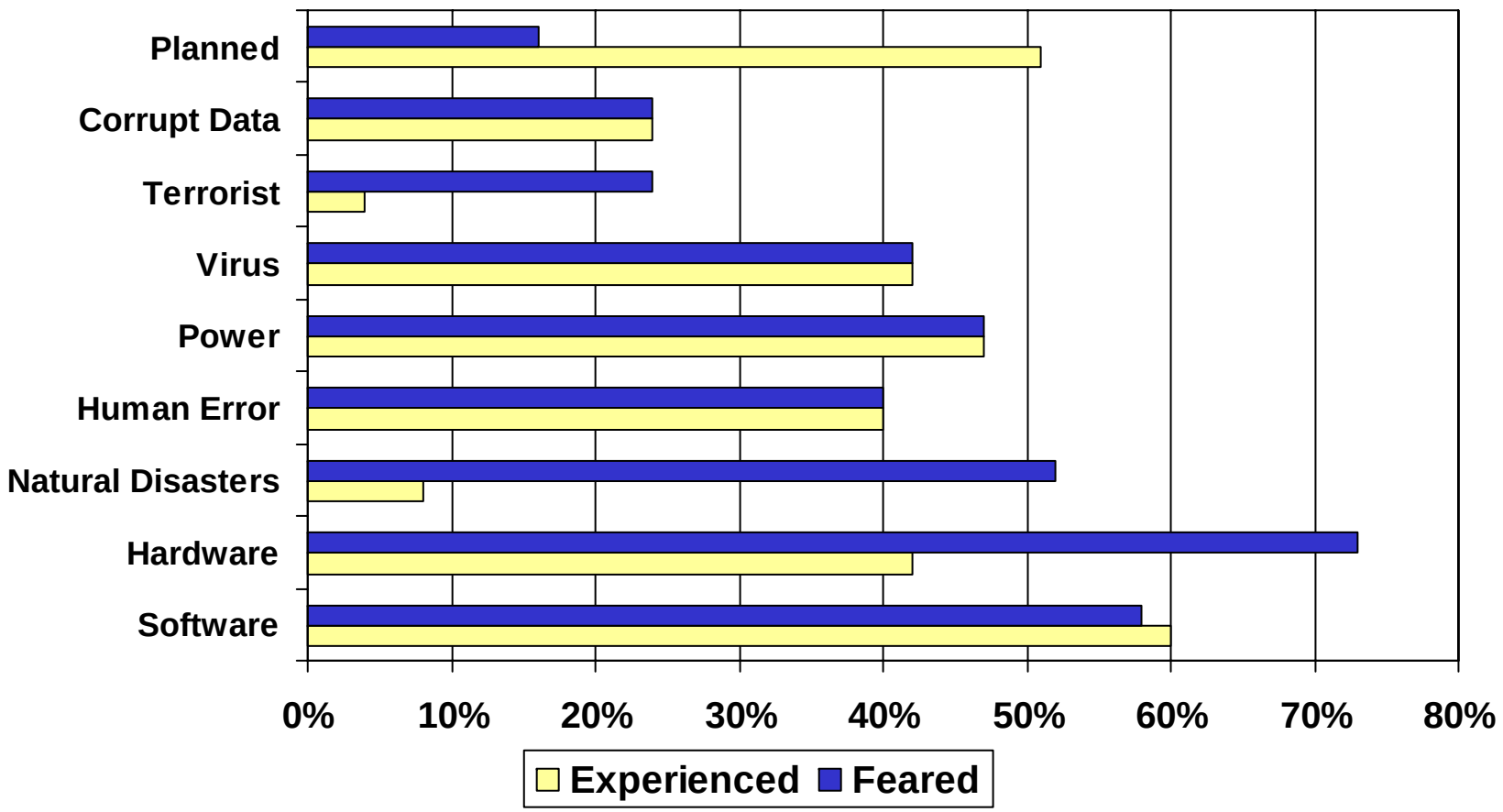
State of Business Continuance

- Case Study: large company with real-time switch over to Business Continuity site
  - Dedicated Security staff with documented security policy
  - Was notified on worm and reminded to patch servers
  - Decided to wait until next scheduled patch run
  - 50 servers got infected and the systems started rebooting every 60 seconds
- Infection didn't come from the Internet
  - Worm was brought in on a users laptop
- Business continuity site must be protected from internal spread of viruses and worms
  - Ingress and Egress IDS systems

State of Business Continuance



State of Business Continuance



State of Business Continuance

- **Ten common effects of a computer disaster:**
  - Loss of business/customers
  - Loss of credibility/goodwill
  - Cash flow problems
  - Degradation of service to customers
  - Inability to pay staff
  - Loss of production
  - Loss of operational data
  - Financial loss
  - Loss of financial control
  - Loss of customer account management

State of Business Continuance

- **Business Continuity site should be protected from virus/worms from internal sources**
  - Most sites pass authentication information (Active Directory, LDAP, etc.)
- IDS/IPS should be used between endpoints
  - Mirage networks has an internal IDS/IPS product
  - Limit traffic between production network and Business Continuity to very specific traffic

State of Business Continuance

- '"For many real-time enterprises, a four- to 24-hour site outage would cause irreparable damage to the enterprise,'" said Donna Scott, vice-president and research director for Gartner. "Because the risks are greater with real-time enterprises, the business continuity plan must address new scenarios, and BC processes must integrate with a greater number of enterprise processes."
- '"With real-time enterprise applications, it is critical that business continuity be built into the life cycle for new applications and business process enhancement projects so that availability and recovery requirements are built into the architecture and design,'" said Scott."

CyrusOne

State of Business Continuance

- For many companies ‘Business Continuity’ only provides value if a natural disaster arises
- Business Continuity should be used when primary production systems have been impacted (security/worm issues, hardware issues)
- If you’ve ‘engineered’ a business continuance solution then it could bring value supporting your production environment

State of Business Continuance

- E-Bays move to Business Continuance
- Outage in ’99 caused them to redesign their design
- Re-architected the sited while on-line and processing transactions
- Old environment was 4 to 5 large databases that updated every 6 to 12 hours, 60 front-end IIS servers and ISAPI servers
- Database servers used to have 10s of processors on each server

State of Business Continuance

- New design is spread across 4 data centers (each data center can support around 55% of the load)
- E-Bay can lose any two data centers and still handle full load (the design was built to support 200% of the current load and to scale)
- Now they have 200 databases (50 at each data center) and they update each every 90 seconds
- Servers have 6 to 12 processors
- Content Networking pushes traffic to the nearest active data center

State of Business Continuance

- E-Bay's partners in the design were: Sun for the server hardware, Hitachi data systems for the storage, Brocade for the fiber channel network, Oracle, Microsoft and IBM
- Most companies cannot afford the type of architecture that E-Bay has put together
- Most companies can accomplish the same type of redundancy utilizing different hardware/software

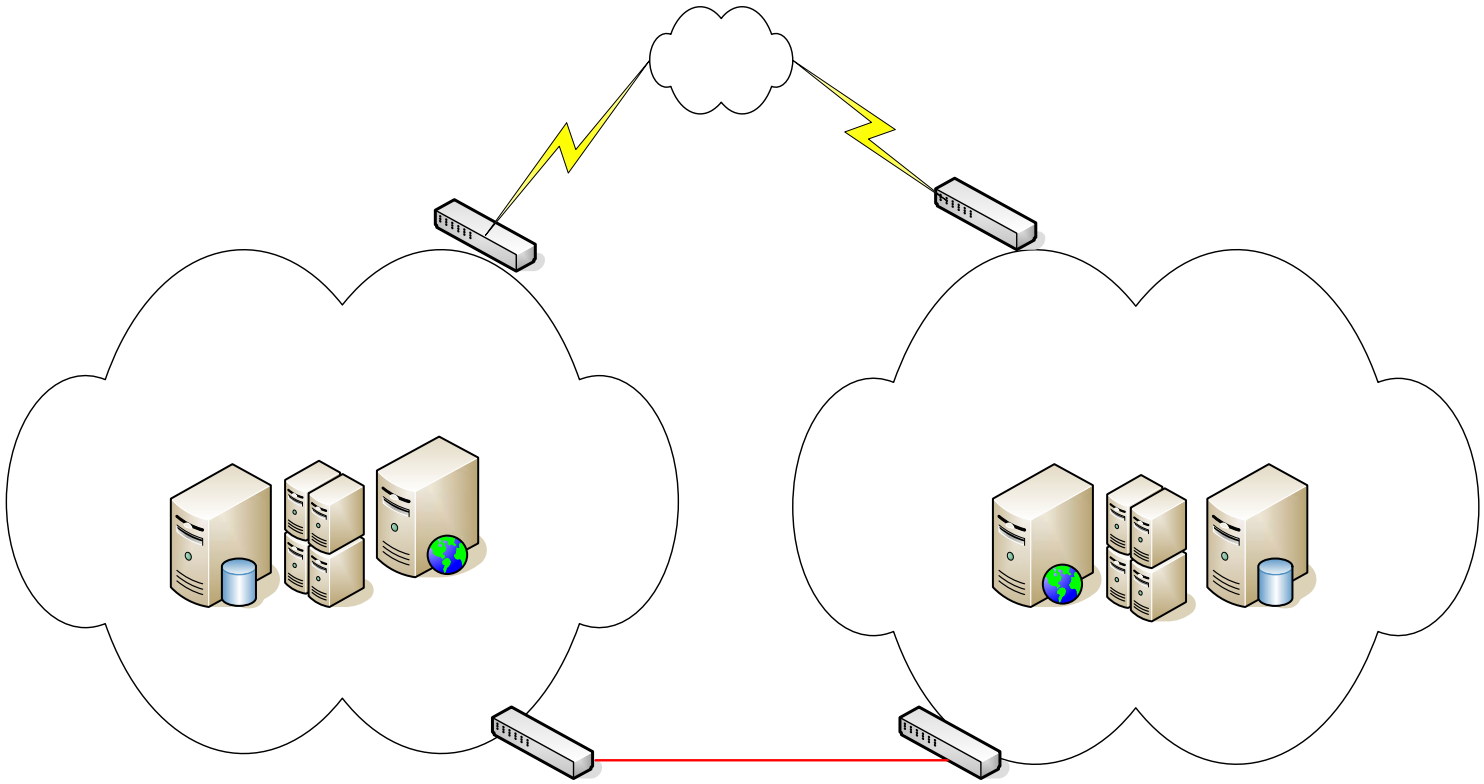
State of Business Continuance

- E-mail is one of the most critical applications for most companies
- There is inadequate failover for most companies
- Majority of companies have to rebuild e-mail systems and then point the mail client to the new mail system
- Failover to a WAN clustered environment is usually very expensive (or at least used to be)
- Exchange could be mirrored to another site and the remote-site's Exchange could automatically take over when the primary site goes down and fall back when the primary site comes back up
- Same for the MS SQL Database or file system

State of Business Continuance

- Replication/Failover Software (XOSoft, Steeleye, Neverfail, etc)
  - At least one of the above products fails over ‘automatically’ and users don’t have to point to a different mail server
  - Makes a change to Active Directory
  - Can be used across a WAN
  - Automatically fails back over
- Works for MS SQL, as well
- What used to be available for only SANs environments is now available at reasonable prices

State of Business Continuance



Using the Web

- Whether applications are web enabled or not, the web can provide access
  - Reverse Proxy systems (Safeweb Tsunami, for example)
  - Citrix
- Security can be provided by VPNs, SSL, etc.
- More business continuity flexibility (customers and internal users)
- There are a considerable amount of tools available for monitoring security, web performance

Using the Web

- Security Policy has to be documented and enforced
- There are companies that have never experienced downtime due to a virus or worm
- More business continuity flexibility (customers and internal users)
- There are a considerable amount of tools available for monitoring security, web performance, etc.

Using the Web

- Simplifies business continuity solution
- Majority of companies and a large segment of the population have Internet connectivity
  - 203,271,187 Internet users as of June/04, 69.3% of the population, Nielsen//NR.
- With the proper configuration/appliances, customers may not even know that your production environment has taken a hit
- Customer connectivity doesn't change

Keeping it Local

- MasterCard realized that having its Business Continuity facility in New York was a serious issue
  - They may not be able to get their people to the facility during a disaster
  - Testing of a Business Continuity plan when the facility is clear across the country was an additional issue
- Master card moves its Business Continuity facility closer to its HQ
- More companies are following suit

Keeping it Local

- Understand the type of disasters that can occur
- Identify the type of disaster or issues you want to mitigate
- Look at the company outage history, and identify the type of outage and duration
- Look at resources (support staff, systems, regulations, etc.)
- Identify true outage numbers. For example, a 10 minute power failure could cause an hour or more of downtime (dependent upon getting systems backup and operational)

Keeping it Local

- Skill sets (employees) may not be willing to go out of town if their family is impacted by a natural disaster
- For shorter outages (those of under 6 hours), having a redundant facility 300 miles away or more does a company very little good
- Companies are more apt to test a Business Continuity plan if the redundant facility is local
- Hardware and software upkeep/maintenance of Business Continuity systems is easier if the redundant site is local

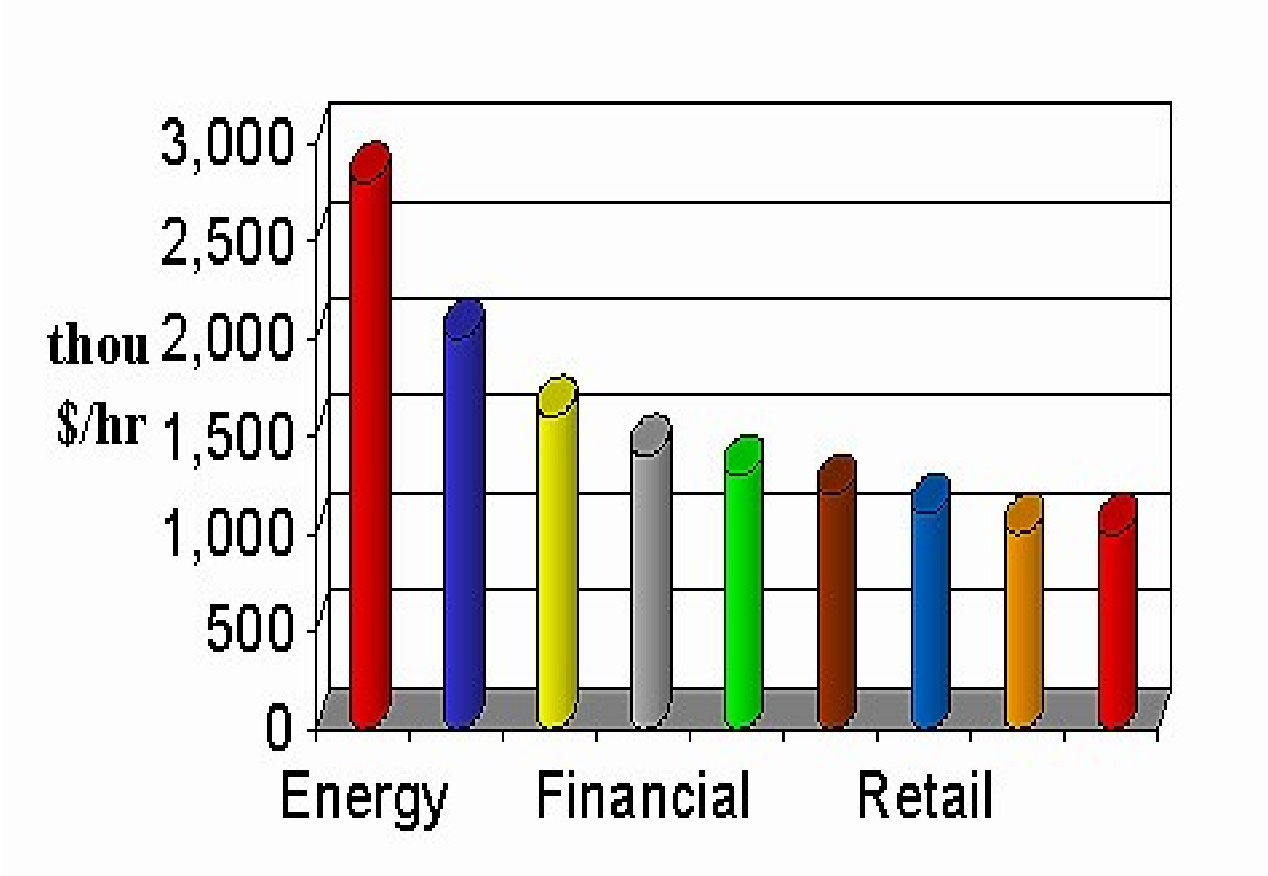
Business Continuance

- Understand the risk and what issues you are trying to mitigate
- Plan and Engineer a solution
- Utilize the web for access
- Strong Security Policy
- Utilize the Business Continuance solution as needed (for short duration outages or significant increases in traffic)

Downtime Statistics

- According to industry statistics, 87% of all businesses that encounter major data disruption without a viable, working business continuity strategy will be out of business within two years.
- 80% of all disruptions occur due to non-disaster related events by either hardware failure or operational errors caused by people.
- META Trend: By 2008, 45% of Global 2000 users will utilize two data centers to deliver continuous availability; of these, 25% will support real-time recovery. By 2006, more than 60% of G2000 data centers will utilize capacity on demand to satisfy less critical recovery services. Through 2008, more than 50% of G2000 users will utilize a single "hardened" data center augmented by third-party services to deliver traditional, cost-effective disaster recovery services (48- to 72-hour recovery).

Downtime statistics



Conclusion

- Business Continuity is becoming increasingly inexpensive
- Engineer with Business Continuance in mind
- Identify your goals
- Identify what type of outages you have been experiencing and their duration