Disaster Planning and Recovery BOF

Internet2 Member Meeting, Chicago
11:45AM, December 4th, 2006
Room CC24C

Old DR Paradigm

- Reciprocal shared space at a partner site
- Data archived to tape
- Just-in-time delivery of replacement hardware
- Small number of key applications (typically enterprise ERP system)
- Down time acceptable
- Proforma/low probability of occurring
- Is that still a realistic paradigm? NO.

What **Risks** Are We Worried About Today?

- Equipment failure? (should this now all be getting handled by system architectures?)
- Point failure/attack? (such as a facility fire, perhaps as a result of an arson)
- Regional natural disasters? (such as a hurricane)
- National scale cyber attacks? (a major worm, for example)
- Something else?

What's Mission Critical?

- Domain name system?
- Enterprise SAN/NAS (data storage)?
- Enterprise Identity Management System?
- ERP System?
- Teaching and Learning System?
- Institutional Web Presence?
- Email and Calendaring?
- The network itself?
- All of the above and more?

What Are Today’s Restoration/ Recovery **Time Frames**

- Hitless/non-interruptible?
- Restoration on the order of seconds?
- Minutes?
- Hours? <== I suspect this is what we need
- Days?
- Weeks? <== Is this where we are?
- Longer?
- **Assertion: time to recover is a key driver.**

Key Driver? **Total Data Volume**

- How many GB/TB/PB worth of data needs to be available post-event?
- If that data needed to be transferred over a network or restored from archival media post-event, **how long would it take to do that?**

Key Driver? **Data Change Rate**

- If restoration has to occur from a checkpoint/periodically archived media, how much data would be at risk of loss since that snapshot?
- Are the transactions which occurred since that time securely journal'd, and can they be replayed if need be? Or would those transactions simply be lost?

Key Driver? **Required Lower Level Infrastructure**

- Secure space with rackage
- Power and cooling
- Local loop and wide area connectivity
- System and network hardware
- How long would it take to get/install/configure that lower level infrastructure from scratch, if it isn’t already there?

Key Driver? **System Complexity**

- Today’s systems are complex.
- Replicating complex systems takes time and may require specialized expertise
- Specialized expertise may not be available during a crisis
- Debugging a specialized system may take time…

Key Driver? **Cost**

- Facilities themselves? (NOT cheap)
- Hardware? (commodity PCs are cheap, but enterprise-class SAN/NAS boxes are NOT)
- Software? (ERP licenses are NOT cheap!)
- Staff? (Personnel costs often dominate IT budgets -- what would staff impacts be?)
- Network connectivity? (Function of facility separation distance, bandwidth required, and redundancy demands)

Strawman Proposal/Suggestion

- **Doing disaster recovery/business continuity today requires a hot/spinning off site facility with synchronized data.**

Testing

- When it comes to disaster recovery and business contunity planning, the key to making this real is going to be testing the plan. Give yourself an **intentional** disaster!
- Hypothesis: many sites do not and will not test (and probably for dang good reasons)
- That’s probably a sign we have a lot of work to do!