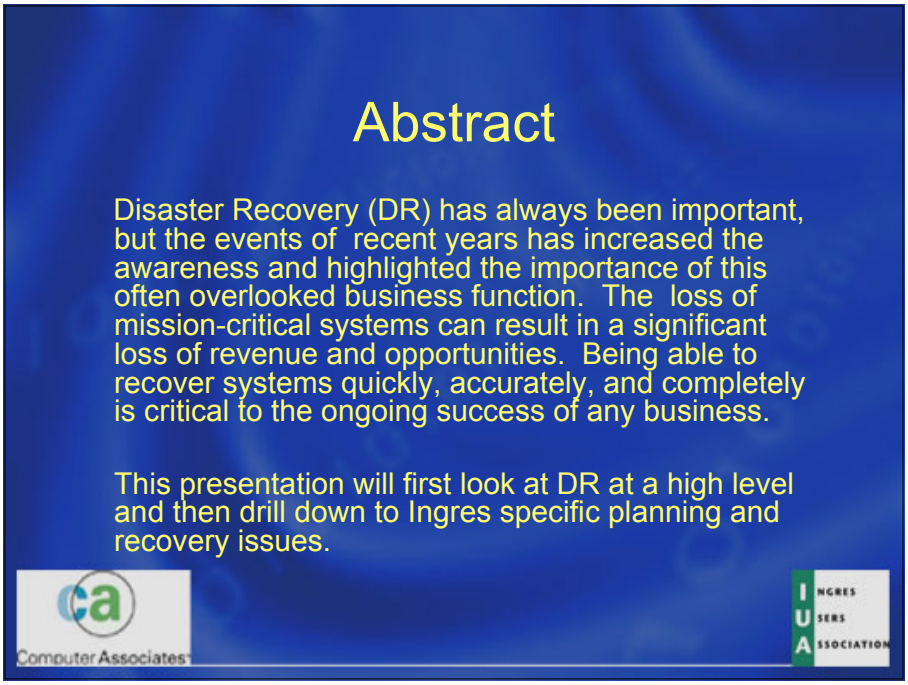


Biography

- Chip Nickolett
- Comprehensive Consulting Solutions, Inc.

Chip is the founder of Comprehensive Solutions (www.Comp-Soln.com), was a Senior Consultant for the Ingres Products division of the ASK Group, and was both a Consultant and Consulting Manager for Computer Associates. Chip is also a past President of the North American Ingres Users Association (www.naiua.org). He has worked on DR projects for the past 10 years in various environments.

Topics of Discussion

- What is Disaster Recovery (DR)?
- Typical Approaches to DR
- Where to Start
- Typical DR Plan
- Ingres Specific Planning
- Download Samples & Other Information
- Summary

Words of Wisdom

Dramatic change often comes as a response to imminent collapse.

-- Tom Peters

Strategy is not the consequence of planning, but the opposite: its starting point.

-- Henry Mintzberg

What is Disaster Recovery?

- Typical Response – **System Recovery**
  - But what systems?
  - Recovered to when?
  - Isn't this what backups are for?
- A better response is: *Disaster Recovery is the coordinated process of restoring systems, data, and infrastructure required to support key ongoing business operations.*

What is Disaster Recovery?

- "**Systems**" include both hardware and software
- "**Data**" includes true data, log files and audit information, as well as "business knowledge" (such as procedures and business rules)
- "**Infrastructure**" includes phones, office space, remote access, intranets, websites, firewalls, etc.
- "**Business Operations**" are the things that your business does on a daily basis to generate revenue

Computer Associates

IUA Ingres Users Association

Typical Approaches to DR

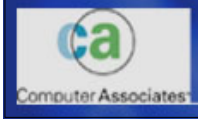
- **Hot Sites**
  - Need to maintain redundant environments
  - Use of Storage Networks (SANs) is ideal from a technical perspective
  - Replication or restore from current backups are two other commonly used techniques
  - Generally provides the benefits of proximity and availability
  - A true "hot site" is generally the most expensive, fastest to recover, and most reliable approach

Computer Associates

IUA Ingres Users Association

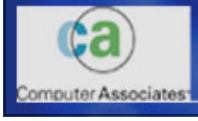
Typical Approaches to DR

- **DR Facilities & Service Providers**
  - Cost is "fixed" over length of the contract
  - The cost for testing may be extra
  - Contracts may lack absolute guarantees and/or service level agreements (SLAs)
  - Hardware configuration issues common
  - Availability issues may occur
  - Possible Bandwidth / Accessibility issues
  - Are they committed to your success?



Typical Approaches to DR

- "We will just restore from backups"
  - Where will the restore occur?
  - Are you sure the backups are good?
  - Will the data from disparate systems be in sync?
  - What about offsite backups that are older?
  - Will the equipment be compatible?
  - What about remote access, network bandwidth, data security?
  - What about *Running the Business*?



Where to Start

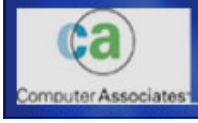
- **Create a DR Team**
  - Executive Sponsor
  - DR Coordinator
  - Team Leads and Members
  - Need to define both primary and backup contacts for each team position. The goal is to not have any person become a "single point of failure"

Where to Start

- **Identify Business Requirements**
  - Requirements are different than Goals!
  - Identify functional areas to be recovered (for example: locations, lines of business, specific functionality)
  - Categorize those systems into Tiers
    1. Recover ASAP - generally within hours
    2. Recover within days or weeks
    3. Recover within a month or more

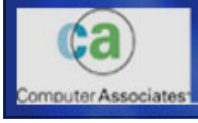
Where to Start

- **Identify Business Requirements (continued)**
  - Define the Recovery Time Objective (RTO). This is the goal for having the Tier 1 systems operational.
  - Define the Recovery Point Objective (RPO). This states how much data can be lost based on time from the point of failure going backwards.
  - Set expectations based on this common understanding of the business goals!



Where to Start

- **Identify & Categorize Risk**
  - What is the most likely to occur?
    - Fire?
    - Natural Disasters such as an earthquake, flood, tornado or hurricane?
    - Loss of infrastructure (power, network, facilities)
    - Terrorism? Hackers? Other “evil”?
  - Look at the probability and cost of each type of disaster, determine the “business adjusted risk” and then plan accordingly



Where to Start

- **Identify Critical Systems**
  - Key processes and applications
  - Dependencies on other systems
  - Interaction with other systems
  - Manual processes and intervention
  - Are there any business or legal requirements for this system (FDA, DoD, ISO 17799, NFPA 1600, HIPAA, Gramm-Leach-Bliley Act, Sarbanes-Oxley Act, etc.)? **If so you need to ensure compliance on an ongoing basis!**

Computer Associates

INGRES USERS ASSOCIATION

Where to Start

- **Identify Key Personnel**
  - May not be part of the DR Team!
  - Identify Roles and Responsibilities
  - Associate Names with the Roles
  - Have a clear policy defined regarding who has authority to do what
    - For example, who can declare a disaster and under what circumstances?

Computer Associates

INGRES USERS ASSOCIATION

Where to Start

- **Identify Single Points of Failure**
  - The goal is to mitigate unnecessary risk, *within reason*
    - Identify Single Point of Failure (SPOF) items
    - Estimate the Probability of Failure
    - Estimate the Number of Incidents per year
    - Estimate the Cost per Failure and the Annualized Loss Expectancy (ALE)
    - Compare the Cost of Mitigation to the ALE

Computer Associates

INGRES USERS ASSOCIATION

Where to Start

Single Points of Failure Project
Failure Analysis Overview

Last Update: 10/08/2002

Tracking #	Business Areas Affected	Impact (1=low, 5=high)	Probability of Failure (1=low, 5=high)	Single Event Loss Expectancy ($/Incident)	Estimated # of Incidents per year	Annualized Loss Expectancies ($/year)	Estimated Cost of Mitigation	SPOF Item
1	Entire Company	5	1	$278,066	0.25	$69,517	$5,600	Networking (and phone) equipment in Telecomm closet does not have redundant UPS support
2	Entire Company	5	1	$278,066	0.2	$55,613	$66,439	Cisco 6509 network backbone switch is not redundant
3	Entire Company	5	1	$278,066	0.2	$55,613	$15,000	Relocate redundant network equipment to a separate physical rack
4	IT - All	4	3	$16,000	1	$16,000	$80,000	Primary Development platforms do not have failover platforms.
5	Entire Company	4	3	$16,000	0.5	$8,000	$122,000	Computer room does not have sufficient UPS capacity to run on a single unit
6	IT - All	2	2	$1,600	1	$1,600	$20,000	eRooms system does not have a failover platform.
7	IT - Intranet / B2B	2	1	$3,600	0.5	$1,800	$5,000	There is no failover platform the development webserver
8	IT - EDI	2	1	$400	1	$400	$10,000	EDI development platform lacks a failover platform

Computer Associates

INGRES USERS ASSOCIATION

Typical DR Plan

- **A Project Plan that works**
  - Just because it looks impressive in MS Project doesn't make it a good or valid plan!
  - Shows critical systems
  - Shows dependencies, helps identify overlap
  - For most sites the plan should be at a higher level, pointing to detailed recovery procedures

Computer Associates

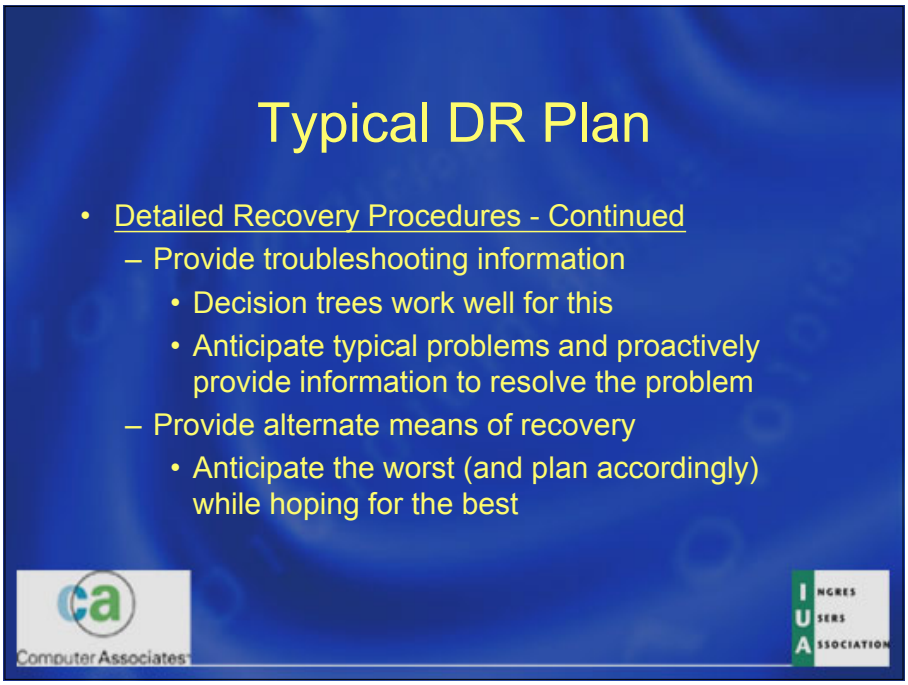
INGRES USERS ASSOCIATION

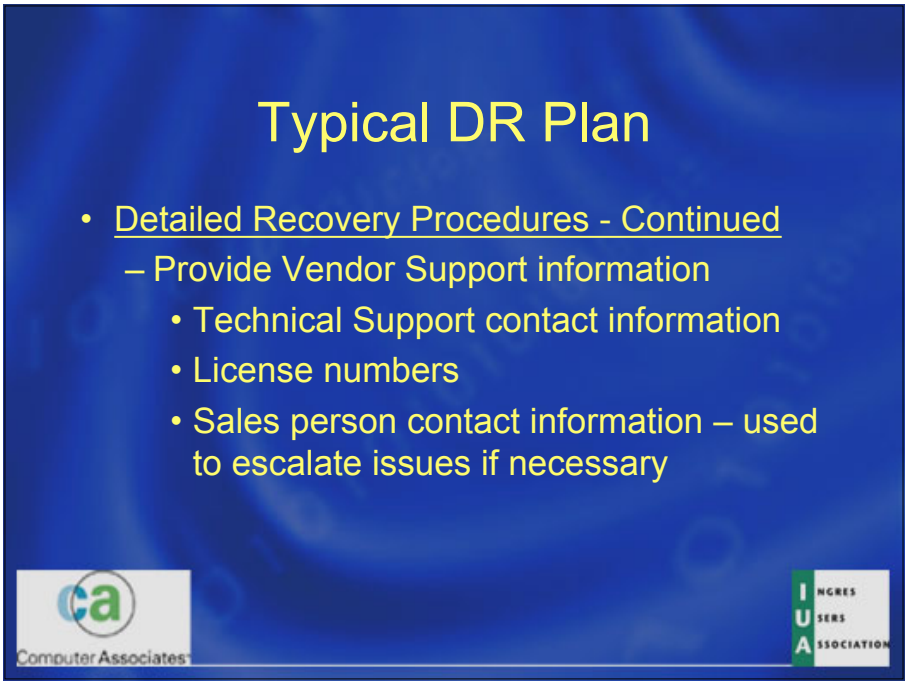
Typical DR Plan

- **Detailed Recovery Procedures**
  - Design the procedure to be used by someone who is not an expert with the system being recovered
  - Provide specific commands and representative output from those commands
  - Provide check boxes and an area to write in time started / completed and comments
  - Cross-training provides both depth of coverage and validation of the process

Computer Associates

INGRES USERS ASSOCIATION





Typical DR Plan

- **Detailed Test Plans**
  - Need a way to validate that critical systems have been fully and properly recovered
  - Need to validate external access, access to dependent systems, data feeds, etc.
  - Will ideally provide the means to validate the accuracy of the data
  - Provide basic performance validation

Typical DR Plan

- **Detailed Security Plan**
  - What needs to be secured and why?
  - Can secure and non-secure data “co-mingle” on a network?
  - Physical security and safety issues should be addressed
  - By what means will people be accessing these systems? Will the connection be secure?
  - Use of production passwords may be a concern at third-party recovery test sites

Typical DR Plan

- **Plan to Restore Operations**
  - In a true disaster the recovery site may be used for weeks or even months
  - Eventually the original operational site will be restored or rebuilt, at which time the recovery site will become unnecessary (or at least secondary)
  - Typically a “Reverse DRP” is used to restore the systems to their final production location

Typical DR Plan

- **Post-test clean-up**
  - Remember, the restored systems are now de facto production systems
  - The systems should be thoroughly “scrubbed” once testing has been completed
  - Failure to do that may result in someone from some other company having access to your production data!

Typical DR Plan

- **Standard Method to Define Success**
  - We use a "Critical Success Factors" spreadsheet that uses weighted values assigned to various systems, functionality, and dependencies
  - Provides a way to demonstrate success and point out areas for improvement
  - Provides a means of tracking both progress and complexity of the overall plan
  - It also highlights flaws and problems due to its use of weighted values and dependencies

Computer Associates

IUA Ingres Users Association

Typical DR Plan

- **Standard Review Process**
  - Identify what went right and what went wrong - identify "lessons learned"
  - Determine why things went wrong and improve the process
  - Look for other opportunities for improvement
    - Efficiency
    - Integrity
    - Automation

Computer Associates

IUA Ingres Users Association

Typical DR Plan

- **Test, Validate, and Refine**
  - Requires full scale recovery tests on a regular basis
  - Staff should be rotated as a means to verify the accuracy and ease of use of the recovery procedures
  - Failure to do this will result in providing a false sense of security!

Ingres Specific Planning

- Gather **OS** specific information
  - kernel / OS tuning parameters
  - disk configuration (df -k)
  - user & group information
  - OS version & patches applied
  - cron jobs (crontab file)
- It is important to know how to rebuild the system - don't assume that the Systems Administrator will have all of this detail (even though they should)

Ingres Specific Planning

- Gather Ingres **Installation** Configuration Information
  - Customized files (termcaps, checkpoint templates)
  - config.dat, protect.dat, and symbol.tbl
  - ingprenv output redirected to a file
  - version.rel
  - The license file (/ca_lic/ca.olf)
  - select * from iiusers; (from iidbdb)
  - select * from iiusergroup; (from iidbdb)
  - select * from iiroles; (from iidbdb)
  - select * from iirolegrants; (from iidbdb)

Computer Associates

INGRES USERS ASSOCIATION

Ingres Specific Planning

- Gather **Database** Specific Configuration Information
  - "unloaddb -c" and "infodb" output
  - select * from iitables
  - select * from iifile_info
  - select * from iimulti_locations
  - help table *
  - help index *
  - "aaaaaaaa.cnf" & "aaaaaaaa.rfc" (may not exist) from the ii_database directory for each database
  - "aaaaaaaa.cnf" from the ii_dump directory

Computer Associates

INGRES USERS ASSOCIATION

Ingres Specific Planning

- **Prerequisite Step – Restore Server (Mirror Production Configuration)**
  - User Accounts and Groups
  - Filesystems (empty)
    - Size
    - Ownership
    - Mount points / paths
  - Any critical directories
  - Specific files that have been customized
  - OS kernel parameters & patches

Computer Associates

INGRES USERS ASSOCIATION

Ingres Specific Planning

- **Licensing & Support during a disaster**
  - Contact CA Technical Support to make them aware of the situation in case you need help
  - Request a temporary license file (ca.olf)
  - Advantage Ingres 2.6 no longer uses the “MAC” address of a machine, so the license file should work on a new machine that is the same hardware platform as production

Computer Associates

INGRES USERS ASSOCIATION

Ingres Specific Planning

- **Restoring the Ingres Installation**
  - OS Backup is generally fine
    - Also helps minimize problems related to customized files such as termcaps and checkpoint templates
  - Be prepared to reinstall Ingres
    - Implies that both the installation media and the patch media (for the patch version used in production) is readily available

Computer Associates

IUA Ingres Users Association

Ingres Specific Planning

- **Restoring the Databases**
  - rollforwarddb ideal
    - Point in time recovery requires journals and
    - Recovery up to the point of failure requires the transaction log file (SANs really help here)
  - OS Backups & Reload from unloads are a last resort
  - Know your RPO! (recovery point objective)

Computer Associates

IUA Ingres Users Association

Ingres Specific Planning

- **Validating the Databases**
  - Have a well defined means of validating the integrity of the database
    - Table and row counts
    - Aggregate values that can be reproduced
    - Reports of specific activity (such as sales)
    - Overall size of the database

Computer Associates

INGRES USERS ASSOCIATION

Ingres Specific Planning

- **Validating the Environment**
  - Do all required products work?
  - Do Ingres/Net connections work?
  - Are there any unusual errors in the errlog.log file?
  - Do all standard tools and facilities work?
  - Is performance consistent with what you are familiar with?
  - Test to make sure that “restricted access” really is!

Computer Associates

INGRES USERS ASSOCIATION

Ingres Specific Planning

- **Safeguarding the Environment**
  - This is now production – treat it as such!
  - Immediately checkpoint the database(s) and enable journaling
  - Plan for routine care and maintenance of the environment
    - Checkpoints
    - Table modifications

Computer Associates

IUA Ingres Users Association

Ingres Specific Planning

- **Best Practices**
  - Keep multiple copies of installation and patch media offsite (but readily available)
  - Collect important configuration information daily or weekly and save copies offsite
  - Validate your checkpoints on a regular basis
  - Manually remove checkpoint and journal files so that the configuration file (aaaaaaaa.cnf) does not lose knowledge of them.
  - Provide means of validating key data at any point of time (within reason)

Computer Associates

IUA Ingres Users Association

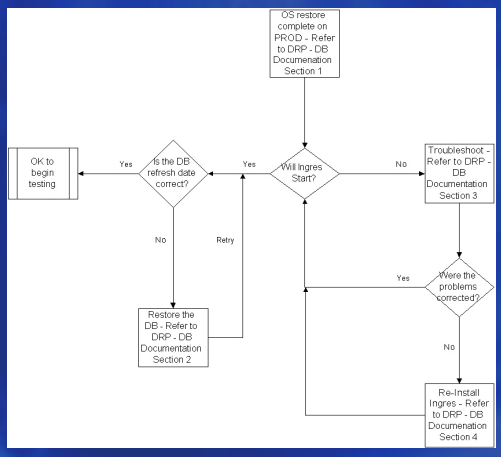
Ingres Specific Planning

- **Common Problems**
  - Ingres Licensing
  - OS kernel parameters and/or patches different
  - Paths not the same
  - "hostname" is different (can be corrected, but it is far easier to make certain it is the same)
  - Ingres/Net password and vnode problems
    - Use hostnames instead of IP addresses when defining vnode entries to minimize problems

Computer Associates

INGRES USERS ASSOCIATION

Ingres Specific Planning



Computer Associates

INGRES USERS ASSOCIATION

Download Samples / Other Info.

- Samples of many of the documents mentioned can be downloaded for free at www.Comp-Soln.com/IngresExpo.html
- Other (free) White Papers on Disaster Recovery and Business Continuity Planning can be found at www.Comp-Soln.com/whitepapers/

Computer Associates

IUA Ingres Users Association

Summary

It is important to understand the true purpose of a DRP / BCP, define specific requirements, determine what constitutes success, and then develop a comprehensive plan to ensure success. This plan will need to be updated and refined over time as your business environment changes. Remember, success does not just happen - it is carefully planned.

Disaster Recovery Planning can be a challenging and expensive undertaking, but it is one that could literally determine the future of your company after a disaster.

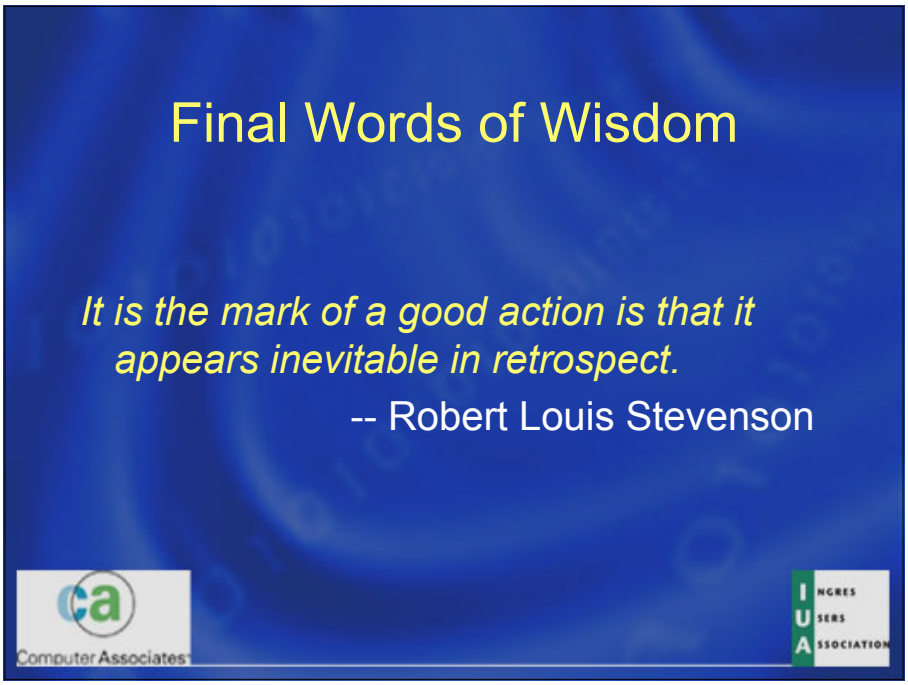
Computer Associates

IUA Ingres Users Association

Final Words of Wisdom

It is the mark of a good action is that it appears inevitable in retrospect.

-- Robert Louis Stevenson



Questions & Answers