Introduction to Dynamic Infrastructure

By Alan G. Labouseur

MARIST SCHOOL OF COMPUTER SCIENCE & MATHEMATICS

MARIST SCHOOL OF COMPUTER SCIENCE & MATHEMATICS

IBM

MODULE 007

BUSINESS RESILIENCY

Introduction to Dynamic Infrastructure

Designed, compiled, written, and edited by
Alan G. Labouseur
www.Labouseur.com / Alan.Labouseur@Marist.edu

Contents

Remarks

Good day, eh? And welcome to week seven. (Sorry. Week 007.)

Nice job on project one. The average grade was 163/200 or 85%. That's not bad.

Project two doing the same analysis for the rest of the DI pillars and adding them to project one so that you have a holistic DI analysis at the end of the class. This means that if project one was less than perfect you will lose points on the first three DI pillars again. (Life's tough. Get used to it.) You can mitigate this by taking time now (as we only have until the end of this month before we're done) to fix up anything that I noted as lacking in project one so that project two is not handicapped.

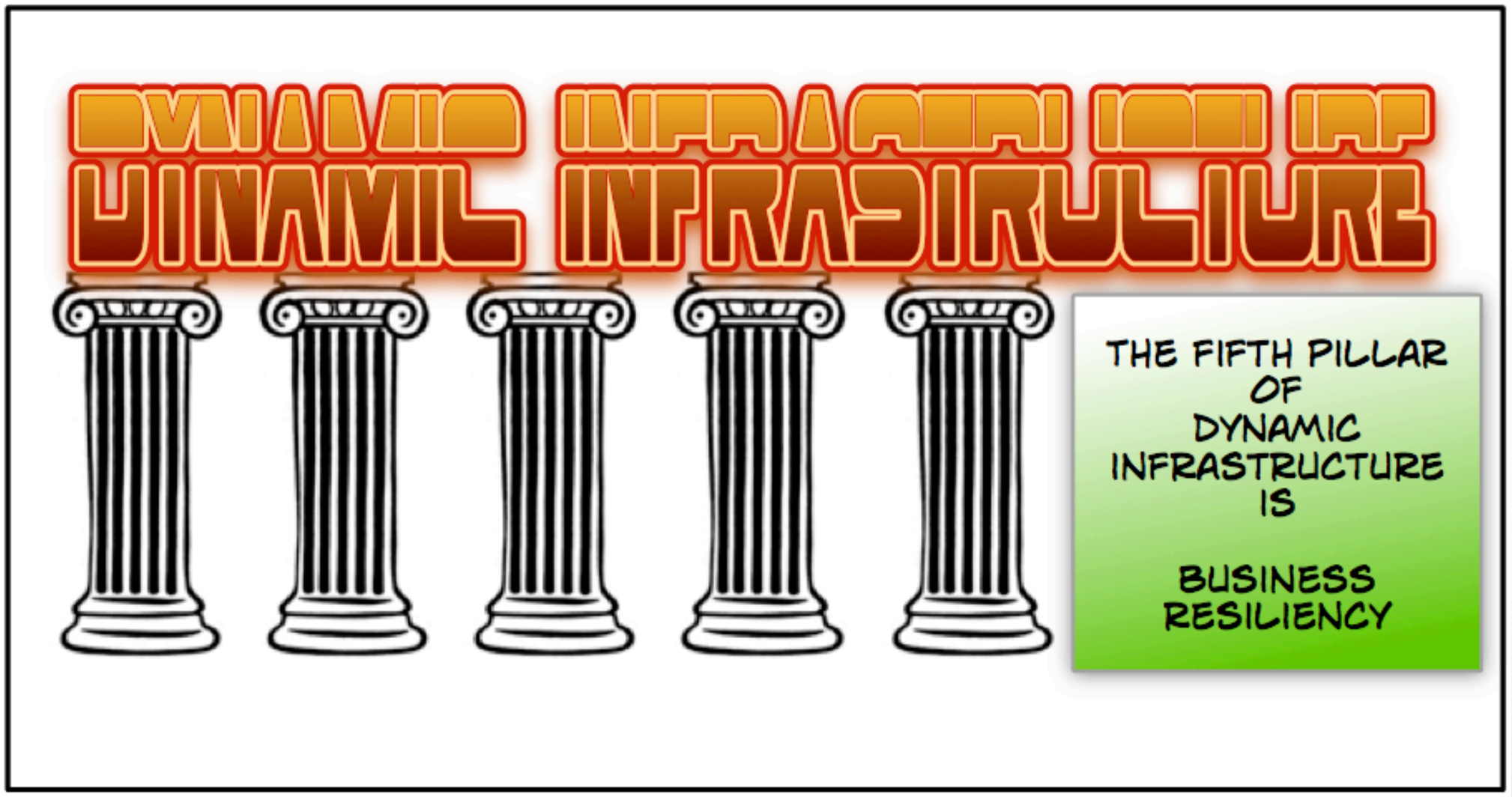
Remember to keep up to date in the Meta forum for details of our field trip on March 25th.

Review

Let's review. Last time our intrepid (and smart) adventurers . . .

- To meet the needs of the business, an approach that contains energy management, virtualization, IT and data center facility services, and server and storage products that are designed to be green
- Technology problems of the IT equipment and the rest of the data center need to be fixed to make them as energy efficient as possible.
- In a data center there is a concept of a hot aisle/cold aisle. Rows of racks alternate one aisle with air intake side, and other aisles with heat exhaust side.
- Cables can reduce and negatively affect air distribution. Some cable congestion can cause hot spots diminishing airflow distribution.
- Measuring estimates the efficiency of the IT equipment, provide a list of applicable energy-saving actions

Business Resiliency



Business Resiliency ?

Business Resiliency is vital to every businesses success. In today's interconnected world, virtually every aspect of a company's operation is vulnerable to disruption.

Some risks could take your business offline for days, but in a competitive environment, even a few hours of downtime could prove fatal. As the number of risks to businesses increases, the worst-case scenario "insurance policy" approach to business continuity has become woefully inadequate.

In a Smart Business Infrastructure you must implement Business Resiliency policies and services which ensure the continuity of business operations and assists with regulatory compliance, improved systems availability, protection of your data, and the integration of IT operational risk management strategies.

Sound hard? It’s a simple matter of B C P.

Business Resiliency ?

Business Resiliency is achieved through Business Continuity Planning (BCP).

BCP is a methodology used to create a plan describing how an organization will resume critical functions either partially or completely which were interrupted within a predetermined time following a disaster or disruption.

Modern BCP Goals:

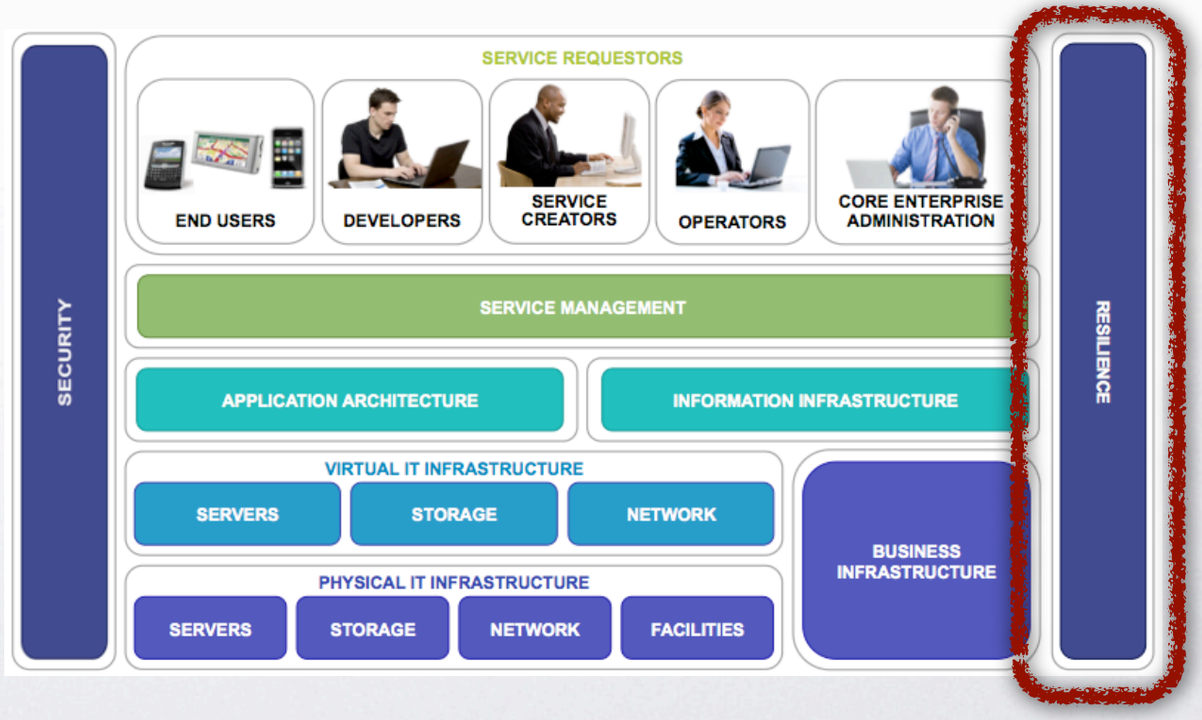
- The old school 72-hour recovery period for business-critical processes is no longer good enough. That's too long in an On-Demand world!
- A new 4 to 24 hour recovery time and recovery point objectives are common today.
- A need for a larger goal of ensuring resumption and recovery of end-to-end enterprise business processes.
- Active/passive configuration between two sites for 30-60 minute recovery.
- 24x7 continuous availability being designed into most critical applications.
- Geographic diversity is imperative

Business Resiliency

Our Plan

- Preparing for a disaster: What's involved? What do we even need to consider?
- Before we can do anything about the various calamities that may befall us, we need to be able to monitor our systems. Otherwise, how will we know when something has gone wrong? So we'll look at Event and fault monitoring.
- Once we have detected a problem, perhaps even a disaster, we'll look at Disaster Recovery (DR) considerations.
- The main tools for BCP and DR are, of course, backup and recovery, so we'll look at those.

The architecture relies on a resilience infrastructure that ensures a consistent timely user experience for each user community.



Business Resiliency > Preparation Questions

Have you developed and documented the appropriate resiliency, availability and recovery strategies for your business?

What actions are you taking to address audit and regulatory requirements from government regulations?

Do you have a plan to protect your mission critical data including the information residing on your employees workstations and mobile computers?

What levels of availability and scalability are required to meet your business objectives?

When was the last time you reviewed and tested your disaster recovery plan in the event of a natural event or system failure?

Business Resiliency > Preparation Strategies

To adequately prepare for workforce continuity during any business disruption, incorporate these five success factors:

- Command and control
  - How will decisions be made and who will make them?
  - What are your plans for succession?
  - How will you interact with local authorities and adhere to possible restrictions in travel?
- Communication
  - How will you exchange accurate and timely information with your workforce and the public?
  - How will you sustain relationships with customers, suppliers and partners needed to conduct business?
- Connectivity
  - How will your workforce regain access to information and technology to resume tasks, possibly at an alternate location?
- Contingency
  - Have you identified critical skills and provided cross-training for crucial roles?
  - How will you ensure continuation of services to your workforce?
- Counseling
  - How will you track the well-being of your workforce during a disruption and provide resources to manage the emotional implications associated with trauma?

Business Resiliency > Preparation Strategies

- Command and Control
  - Consider dividing decision-making responsibility.
  - Incorporate flexibility to adapt to unexpected situations and the various ways these situations could affect your workforce.
- Communication should . . .
  - provide clear direction and establish leadership.
  - offer assurance that you are gaining control and executing a plan to return to normal conditions.
- Connectivity
  - Make sure you provide high-speed Internet access, voice lines and the ability to cross a secure gateway for working from home.
  - Virtualization is another solution to making your organization more resilient and productive. Store a virtual copy of a workers' desktops on a remote servers rather so you can allow access to that desktop from any location.
- Contingency
  - Your workforce continuity plan needs to be flexible and extensible to address specific disruptions
- Counseling
  - Plan to provide critical support services, ranging from healthcare and psychological services to repair services and temporary housing.

Business Resiliency > Event & Fault Monitoring

Monitoring Concepts

- Monitored Element
- Threshold
- Monitoring Rate
- Response Level
- Action

Major Components of an Event and Fault Management Environment

- Monitoring Server
- Monitoring Agent
- Event Management Server
- Event Management Console
- Peripheral Servers
  - Notification
  - Escalation
  - Problem Management

Monitoring events and faults is best done with a control panel. But an eee-vil control panel...?

Event Life Cycle

- Threshold Met
- Agent forwards event
- Event Reception
- Event Processing through Rules
  - Action taken on event
  - Post Event to Console
  - Create Ticket
  - Notification

Interconnections with other areas of Dynamic Infrastructure

- Operations
- Security
- Software distribution
- Availability
- Performance and Capacity

Business Resiliency > Event & Fault Monitoring

Operations Management

- Operations management is the service responsible for directly managing the IT infrastructure based on user experience and event management outputs of an enterprise
- Operators require basic skills of IT elements and usually serve as level 1 support for a variety of probable problems that may occur in the enterprise
- Operators use tools including event management consoles, control book, problem ticketing systems, access to systems for resolution, integration tools, etc.

Some Event Management Tools

- HP IT Operator
- BMC Suite by BMC Software
- Tivoli Enterprise Console
- Netview for z/OS
- Dell OpenManage
- IBM Director

Business Resiliency > Disasters

Disasters are the result of an unforeseen natural or physical event or the consequences of human error.

The current data protection market is characterized by several factors:

- The loss incurred by having data unavailable
- Recovery time frame
- Business continuity strategy (partial or full restoration)
- Level of data protection required by the business

Threats

- Human Error
- Wind
- Earthquake
- Ice storms
- Fire
- Flood
- Cyber attack
- Terrorism
- Civil Disruptions
- Computer Viruses
- Famine
- Pestilence
- War
- Death
- Humun Eror

Business Resiliency > Disasters

Required Reading

Risks

- Power or Communications Outages
- System and/or Equipment Outages
- Governmental or Legal Intervention
- Loss of key personnel

Mitigating the Risks

- Offsite Backups
- Surge Protectors
- Uninterruptible Power Supply (UPS)
- Emergency generators
- Fire prevention systems
- Anti-virus software
- Redundant computing facilities

Bamboo scaffolds have been used in building construction in China for several thousand years.

Business Resiliency > Disasters

Remember the Boy Scouts: Be Prepared

Redundancy is good in servers

- Failover or Clustered processors
- Redundant array of inexpensive disk (RAID) devices
- Dual access paths
- Dual I/O controllers
- Dual power supplies
- Uninterruptible power source (UPS)

Business Resiliency > Disasters

Disaster Recovery Plan - People and things we must consider

- Customers
- Facilities
- Knowledge Workers
- Business Information
- Security of data
- Classification of data for staged recovery

Disaster Recovery Process

- Buy new equipment (hardware) or repair or remove viruses, etc.
- Call software provider and reinstall software
- Retrieve offsite storage discs
- Reinstall all data from back-up source
- Re-enter data from the previous week or latest copy

Business Resiliency > Backups

Backup in computer engineering refers to copying data to a separate media to facilitate the recovery of lost or damaged files, and to protect the organization from a major disaster.

Data recovery is the process of salvaging data from damaged, failed, wrecked or inaccessible storage media when it cannot be accessed normally.

Data backup is done on a defined schedule that ensures the recovery process meets the requirements of the business.

Strategies

- Snapshot Backups
- Full Backup
- Differential Backup
- Incremental Backups
- Continuous Backups (CDP)
- Disk Mirroring

Backup Considerations

- time to completion
- Multiple media backup
- Backup software
- Hardware considerations
- Application/Database Status
- Backup Window
- Backup Resources
- Data Validation

Backup Metrics

- Recovery Point Objective (RPO)
- Backup Window
- Restore Time
- Retention Time
- Backup Validation
- Open File backup

Handling Data Damage

- Types
  - Physical
  - Logical
- Repair Techniques
  - Consistency checking
  - File System Structure Analysis
  - Troubleshooting
  - Component repair or replacement

Data Storage Devices

- Hard disk drive
  - SCSI
  - ATA
- Magnetic tape
- Magneto-optical and optical tape storage
- Optical disc
- WORM

Business Resiliency > Recovery

Recovery is getting back on your feet after a disaster.

Requirements

- Resolution time frame
- Business requirements
- Technical requirements

Recovery requirement documentation

- Desks Manual workaround solutions (interim floor plans and user equipment needs)
- Recovery personnel (short term, long term, specialists, etc.)
- Application and data (All, or categorized by value to the business)
- Maximum outage allowed for the applications
- Peripheral requirements
- Unique business environment requirements

Business Resiliency > Recovery

Recovery Impact scenarios

- Emergency response (protection of life and safety)
- Disaster assessment (identify scope and criticality of the disaster)
- Short term recovery plan (restore critical services)
- Long term recovery plan (restore all services and capabilities)
- Return to pre-disaster operations (fall-back process to return services to the primary data center)

How well is your enterprise prepared? Let's look at seven tiers of disaster recovery and assign a grade:

- F No off-site data
- C Data backup with no hot site
- C+ Data backup with a hot site
- B- Electronic vaulting
- B Point-in-time copies
- B+ Transaction integrity
- A Zero or little data loss
- A+ Highly automated, business-integrated solution

Business Resiliency > Summary of Goals

Manage risk with end-to-end resiliency.

- Adopt a business-driven strategic approach to business resilience.
- Start with a resilience assessment.
- Implement the appropriate business continuity plan.
- Implement an Information Protection Solution to reduce costs, maximize efficiency and protect critical data.

Ensure resilient service delivery.

- Effectively manage risk for key business services in a 24/7 “On-Demand” world.
- Start with a Business Impact Analysis.
- Determine where the current gaps are in continuity.
- Determine where risk to data and inefficiencies lie.
- Implement controls to address disaster recovery compliance requirements.
- Review proactive maintenance policies.

Business Resiliency > Summary of Goals

Reduce cost through proactive incident response.

- Reduce operational costs associated with outages.
- Start with a business risk assessment to understand cost of risk exposures (including compliance).
- Understand resilience optimization solutions to improve responsiveness.

Respond with speed and agility.

- Gain real-time control over risk posture and exposures.
- Determine where risk to data and inefficiencies lie.
- Implement the right resilience strategy for each business process.
- Review sourcing options for flexible response to business needs.
- Review management and monitoring solutions for proactive response.

Business Resiliency > Best Practices

Six Areas to Address:

Strategy

- Prioritization of mitigation actions based on the impact to critical business resources. I.e., risk analysis

Organization

- Provide clarity, definition, and guidance to everybody involved in the enterprise.

Processes

- Prioritize the business processes and establish the mitigation responses needed to protect them.

Data and Applications

- Insure timely, secure, and accurate data backup, validated by prov ing the ability to recover it On-Demand.

Technology

- Virtualizing resources allows for more efficient use of server and data center capacity by provisioning it On-Demand. Cloud computing helps too. It's all part of Smart Business Infrastructure.

Facilities and Security

- Relocation centers must accommodate employees' needs such as child care, living quarters, and health care.

Required Readings

Web Sites

- IBM Business Continuity and Resiliency Portal at www-935.ibm.com/services/us/index.wss/itservice/bcrs/a1000411

Videos

- Tivoli Storage Manager FastBack at http://download.boulder.ibm.com/ibmdl/pub/demos/on_demand_illustrated/Streamed/IBM_Demo_Tivoli_Storage_Manager_FastBack-1-Aug08.html?S=DL

Papers (already linked from the prior slides)

- Preparing the Plan [*pdf*]
- Proactive Measures for Forward-looking Enterprises [*pdf*]
- Expanding and enhancing risk evaluation strategies for better data protection [*pdf*]
- Business Resiliency Best Practices [*pdf*]

Optional Readings

Websites

- Planning for the Worst:
  - http://smallbusinessonlinecommunity.bankofamerica.com/blogs/GeneralBusiness/2010/05/24/planning-for-the-worst
- Business resilience. Ensuring continuity in a volatile environment:
  - http://www.acelimited.com/NR/rdonlyres/784FBA28-B1F5-4BEE-9AB1-D1166567CF12/0/BUS_RESILIENCE_62.pdf
- Tivoli Enterprise Console
  - http://www-01.ibm.com/software/tivoli/products/enterprise-console/
- 8 Ways IT improves small business Resiliency
  - http://www.smallbusinesscomputing.com/webmaster/article.php/3881971/8-Ways-IT-Improves-Small-Business-Resiliency.htm

Papers

- Zurich Business Resiliency
  - http://www.zurich.com/NR/rdonlyres/CC7D96C8-BFE2-4220-92AF-3AF24DD136F8/0/business_resilience_br_20090814.pdf
- Resilient Infrastructure: Improving your business resilience. -
  - https://www-935.ibm.com/services/uk/igs/pdf/wp-resilient-infrastructure.pdf
- The Five Principles of Organizational Resilience - http://datapro.com/resources/103600/103658/103658.pdf

Self-test

Business Resiliency

- What are the five success factors in business resiliency?
- Name five threats of disaster.
- What is the current data protection market characterized by?
- In the case of a power outage within your company, name a few things that could be done to diminish the risks.
- What is operations management?
- Why is it essential for businesses to have backups?
- What are the six areas to address in business resiliency?

Self-test Answers

Business Resiliency

- What are the five success factors in business resiliency?
  - Command and control, communications, connectivity, contingency and counseling.
- Name five threats of disaster.
  - Fire, Death, Human Error, Flood, Terrorism
- What is the current data protection market characterized by?
  - The loss of a business by having data unavailable, recovery time frame, business continuity strategy, level of data protection required by the business.
- In the case of a power outage within your company, name a few things that could be done to diminish the risks.
  - Surge protectors, generators, and offsite backups
- What is operations management?
  - The service responsible for directly managing the IT infrastructure based on user experience and even management outputs of an enterprise.
- Why is it essential for businesses to have backups?
  - In the case of a “disaster”, a backup is used so that you can salvage your businesses datawhen the data cannot be normally accessed.
- What are the six areas to address in business resiliency?
  - Strategy, organization, processes, data and applications, technology, and facilities and security.

Discussions

Discuss the "Critical C's" for business resiliency in general . . .

- command
- control
- communications
- connectivity
- contingency
- counseling

. . . then select one to research in more detail. Write about your deep dive:

- Give a few examples of both successful and unsuccessful outcomes after disaster scenarios.
- Rate each example based on the seven tiers of disaster recovery and explain your rating.
- What additional advice do you have for making that area work better in the future?

Remember our discussion expectations and guidelines.

Acknowledgements

Some of the source material and a few of the graphics in this module came from the IBM World Wide Client Technology Centers's Frank De Gilio.

A TON of additional source material was provided by David Graves and Paul Kontogiorgis of IBM in 2006. There would be little here without it.

- By using these materials you agree to the IBM Terms of Use, found at http://www.ibm.com/legal/us/ .
- The IBM copyright and trademark information webpage is incorporated herein by reference: http://www.ibm.com/legal/copytrade.shtml.

More additional material from:

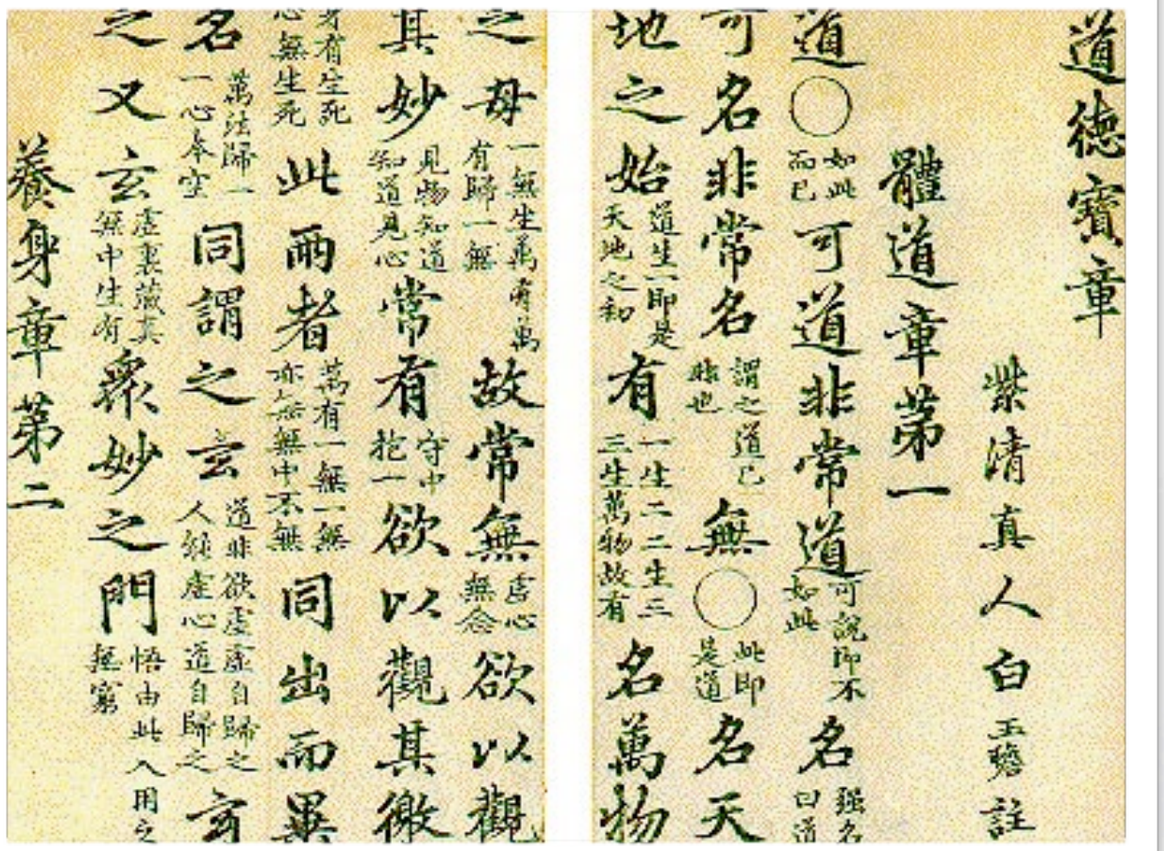
- IBM Business Continuity and Resiliency Portal at www-935.ibm.com/services/us/index.wss/itservice/bcrs/a1000411
- Business Resiliency Best Practices [*pdf*]
- Preparing the Plan [*pdf*]
- Ian Fleming, Stevie Ray Vaughan, and Ted Codd.
- Alan's patient and eagle-eyed student Carley Keefe, who made these slides more accurate and pointed out the worst of the jokes.

007 Gun Logo © 1962 Danjaq LLC and United Artists Corporation. (Ditto the eee-vil control panel.)

Colophon

This work was authored in Keynote by Alan G. Labouseur in July 2010 from his home in Pleasant Valley, NY.

That's the Dao De Jing by Lao Tzu. Though it's a classic work of ancient Chinese philosophy it has much to teach us about technology today.



Distractions that made writing slower:

- WNYC's Leonard Lopate Show podcast
- More of "Under the Dome" by Stephen King
- Fixing my TiVo

Music that made writing faster:

- iTunes Genius Mixes: Classic Rock
- Specific artists: Jazzkantine / Galactic / The Rolling Stones / The Beatles / Earth, Wind, and FIre / Huey Lewis & the News