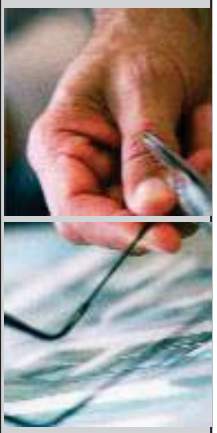


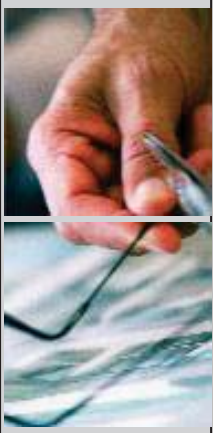
GOVERNMENT FINANCE OFFICERS ASSOCIATION OF MISSOURI

SPRING 2012 CONFERENCE

IT DISASTER PLAN

Presented by:
Scott Wegner
Partner, Director Networking Services
Sikich LLP
1415 W. Diehl Road, Suite 400
Naperville, IL 60563
(630) 566-8417
swegner@sikich.com

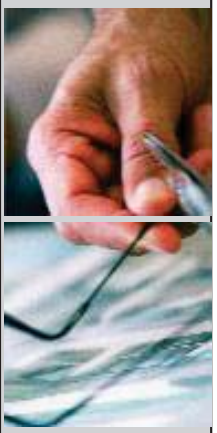
©2012 Sikich LLP. All Rights Reserved.



Objectives

- To provide you with:
  - An understanding of the importance and prudence of Disaster Recovery (DR) planning
  - The processes you need to think about when preparing a DR plan
  - A methodology to create a plan
  - Information on various data backup technologies

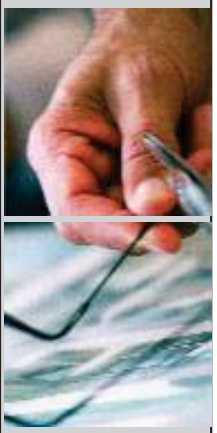
Sikich



Why DR Planning?

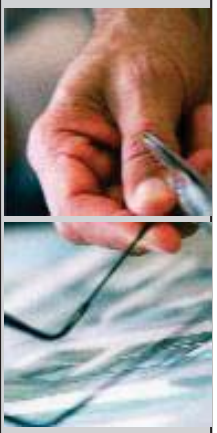
- According to Gartner Group 2 out of 5 organizations that experience a catastrophic event of prolonged system outage never resume operations, of those that do resume operations, 1 out of 3 goes out of business 2 years later
- According to the Department of Labor 93% of businesses that experience a data center disaster fail within 5 years

Sikich



Scary New World – Physical

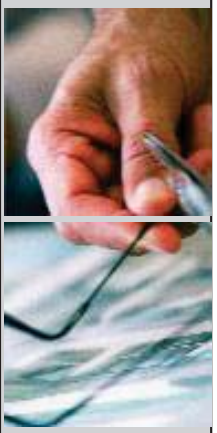
- 9/11 changed everything, and it continues:
  - Anthrax Oct. 2001
  - Northeast blackout Aug. 2003
  - Hurricane Katrina Aug. 2005
- You can no longer assume the public infrastructure would have the necessary redundancy to stay in place
- Can you spell CBRNE?



Scary New World – Regulatory

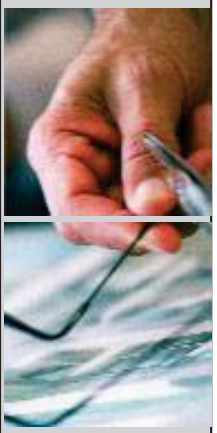
- Regulations makes your data critical to more than just your own organization
  - Sarbanes-Oxley
  - Gramm-Leach-Bliley
  - HIPAA
  - FOIA
  - California Public Law 1386 – privacy regs

  All require information to be available and thusly assumes that it is adequately protected and available when needed



Scope

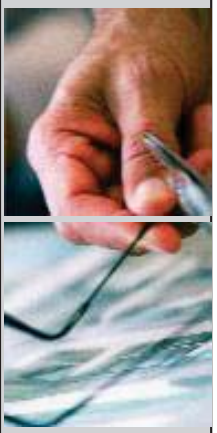
- State and Local agencies cannot afford to have comprehensive plans in place for a total outage or CBRNE
- Focus needs to be on data loss prevention and extended system downtime
- Hot or cold sites might be required
- There are facility needs that should be addressed (not covered today)



It's Not "If" But "When"

- Disaster is defined as an interruption of a system for an unacceptable period of time
- You will have a disaster
  - Most are caused by stupid human tricks
  - You need to plan for a disaster and periodically review and test the plan
- DR is the coordinated process of restoring systems, data and infrastructure required to keep key operations running

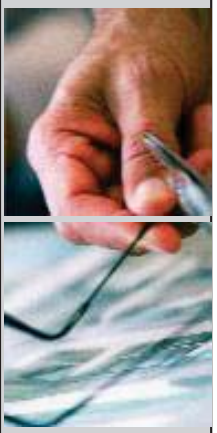
Sikich



Definitions

- Systems – servers, hardware and software
- Data – digital data and the organizational knowledge such as procedures and processes (most of an organization's information is digital)
- Infrastructure – phone systems, electricity, office space, Internet access, etc.
- Operations – the day-to-day processes your organization performs to serve your constituents and staff

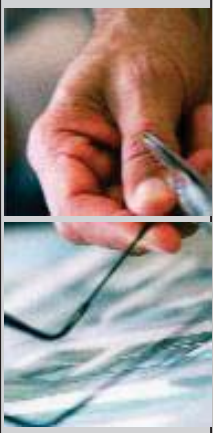
Sikich



Typical DR Plan

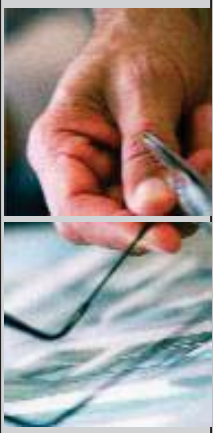
- Backup to tape – “Put a battery on the server and we’ll just restore from tape when we have a disaster!”
- I don’t think so:
  - Are your tapes good? (50% of tape backups don’t work) Are they current? Where are they?
  - What equipment will you restore to?
  - Is virtualization an option?
  - What about remote access?
  - What about running the organization?

Sikich



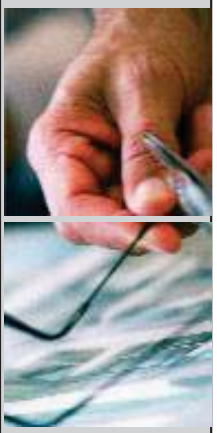
Who's In Charge?

- The responsibility of DR is NOT with the IT department
- The overall responsibility is with a "Chief" – Chief Security Officer, Chief Financial Officer, Chief Operations Officer, etc., reporting to the Executive Director or City Manager
- New regulations mandate CEO is responsible



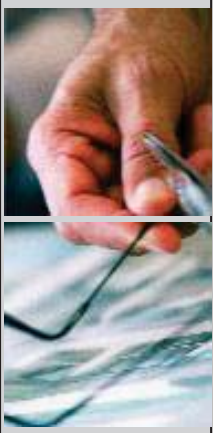
Before We Begin With Planning

- Some critical components:
  - Need buy-in from management and they need to be involved
  - Assign a Project Manager to oversee the creation of the plan
  - Every department needs to be involved
  - Send out a memo explaining the planning to the entire organization
  - Avoid drawn out organizational bureaucracy – create the plan in workshops
  - The planning is ongoing, it is a process
  - Test the plan – if you don't test the plan, the plan isn't done



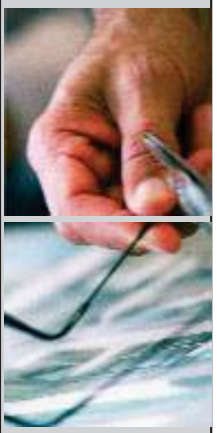
Project Manager

- Building a DR plan is a project and needs a manager:
  - Strong communication skills
  - Broad knowledge of the municipality or agency
  - Understanding of technical environment
  - Consistent follow-up and follow-thru
  - Ability to multi-task
  - Consider use of a committee with one leader



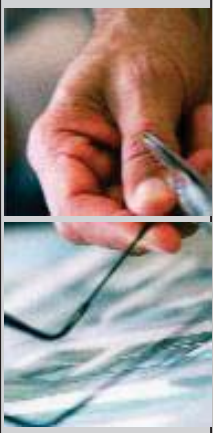
ABC's of the Plan

A. Prioritization of Business Processes
B. Determine Organization Objectives
C. Incident Scenarios Planning
D. Document the Plan
E. Test the Plan
F. Solutions and Other Considerations



Prioritization of Business Processes

- Also referred to as a Business Impact Analysis or BIA
- Segment each significant process in 1 of 3 categories:
  - Mission Critical – core processes required for the running of the operation
  - Organizational Critical – important processes used by your organization, usually across the entire organization
  - Operationally Important – usually limited to individual departments

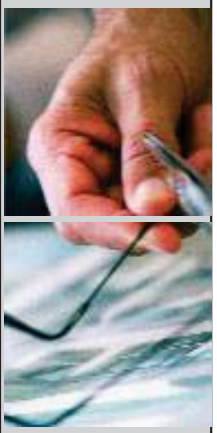


Prioritization of Business Processes

Examples of Categories

1. Mission Critical – constituent facing applications, EDI, community web servers, transaction systems, systems you collect money with, systems critical to your constituents, payroll
2. Business Critical – e-mail, accounts payable, purchasing
3. Operationally Important – HR management, reporting systems, printing, file sharing, office applications

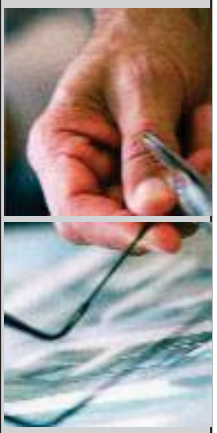
Sikich



Prioritization of Business Processes
Categorizing

- Start small – identify all departments
- Identify key individual(s) in each department with process knowledge
- Keep remote/part-time locations in mind
- Are you dependent on other vendors?
- List all processes and the associated applications and categorize them into 3 tiers
- Get buy-in on the categorization

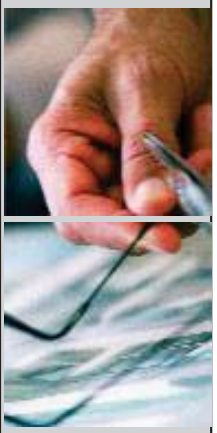
Sikich



Prioritization of Business Processes
How to Prioritize

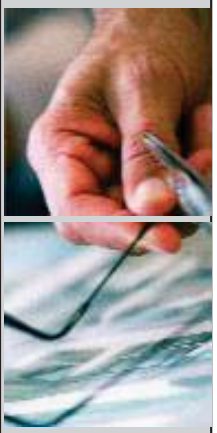
- Things to consider:
  - Consider the impact of the system not being available for an extended period of time
  - How much extra expense would you incur if you lost access to the system?
  - Are there peak periods or seasonal needs?
  - Are there tested work-arounds? Manual processes that can be used?
  - What is being done now to protect the system?
  - Is there any data not being backed up?
  - Is there data that is irreplaceable if lost?
  - What is the cost and impact of reentering data? Can it be reentered?
  - What might you be legally liable for if lost?
  - Impact on image: public, customers, vendors, employees
  - What extra expenses would be incurred if the process was disrupted: temp. employees, overtime, relocation, rental equipment

Sikich



Determine Organization Objectives

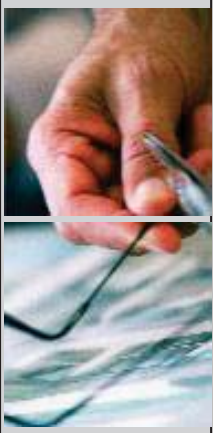
- Data Loss Event (DLE) – type and scope of failure that results in data loss
- Recovery Time Objective (RTO) – the time objective to bring a system back online after a DLE
- Recovery Point Objective (RPO) – the acceptable amount of data loss from the last good backup before the DLE
- Note: You will find that not all data is created equal
- No formula to determine best RTO and RPO, usually there is a negotiation with process owner to balance risk with cost



DLE

- Setting DLE recovery objectives will help process owners categorize their processes (be careful many will want category 1)!

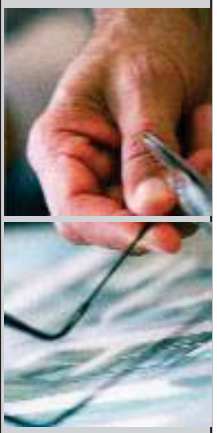
Sikich



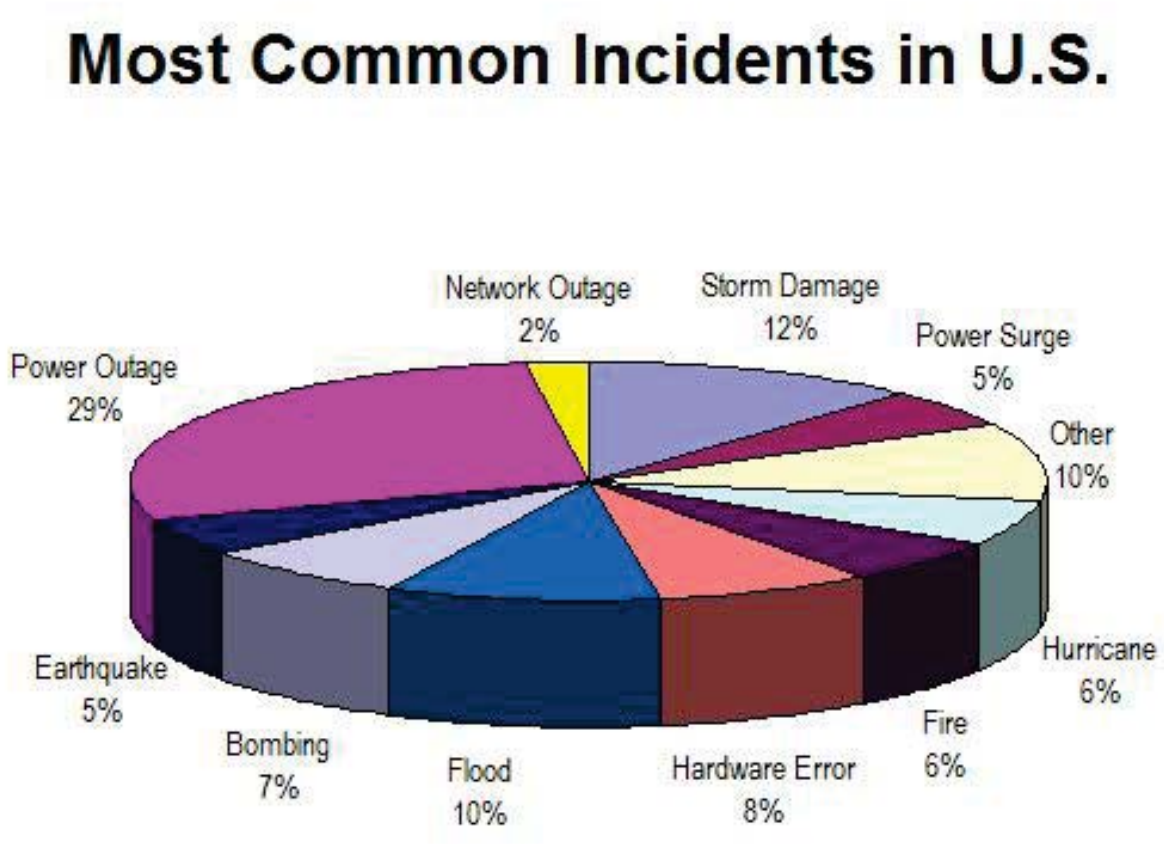
Incident Scenarios Planning
Data Loss

Frequency of most common Data Loss Events

Type of Loss	Description	Frequency
File – human error	Deletion, overwrite, mistakes	83%
File – corruption	Virus, application errors	10%
Storage Loss	Corrupt hardware, malfunctioning hardware	5%
Site	Site disaster – floods, fire, tornados, hurricane, etc.	< 2%
Server	CPU failure, theft, catastrophic virus	< 1%

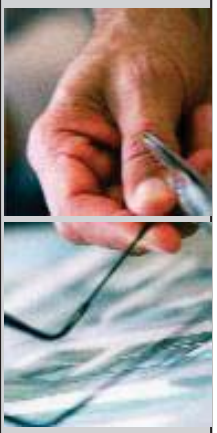


Incident Scenarios Planning
Site Disasters



Source: Contingency Planning Research

Sikich®



Incident Scenarios Planning

Set Company Policy on DLE

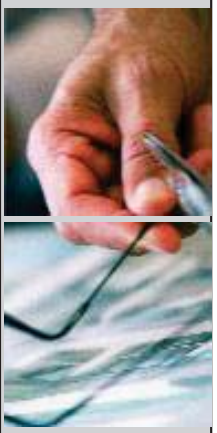
Category	RTO	RPO
Category 1 - Mission Critical		
File loss	4 hrs	15 min
Server loss	24 hrs	15 min
Site	48 hrs	15 min
Category 2 - Business Critical		
File loss	8 hrs	1 hr
Server loss	48 hrs	1 hr
Site	3 days	12 hrs
Category 3 - Operationally Important		
File loss	8 hrs	12 hrs
Server loss	48 hrs	12 hrs
Site	4-5 days	12 hrs

Sikich

Incident Scenarios Planning
DLE Impact by Business Function

Business Function	Impact of Loss	Daily Loss	Rq'd System(s)	Category	Manual Process
Off-line Registration	Revenue	$2K-$7K	Park Rec	2	Y
On-line Registration	Revenue, Service	$4K	Park Rec	2	N
Payroll	Morale, Legal		ADP	1	N
Video Security Cameras	Legal	$?	Sony	1	N
ID Checking	Revenue, Legal	$5K	Park Rec	1	N
Accounting (GL, budgeting, reporting)	Service Revenue	$1K-$5K	Great Plains	2	N
Golf Course Scheduling	Revenue	$10K	Golf Plus	3	Y

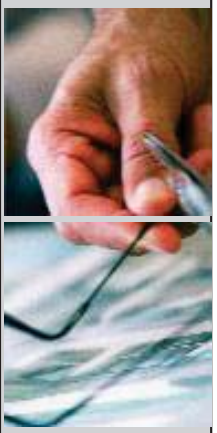
Sikich®



Document the Plan

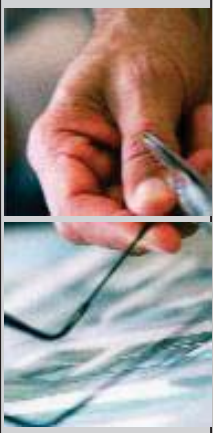
1. Organizational Information
2. Teams and Contacts
3. Recovery Environment
4. Disaster Implementation Tasks
5. Test the Plan
6. Recovery Plan Maintenance
7. Appendices

Sikich



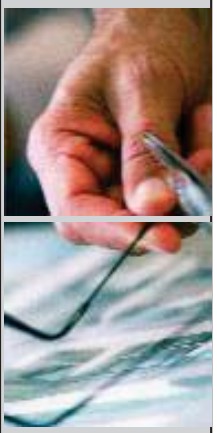
Organizational Information

- Locations covered by plan
- Scope
- Definitions
- Assumptions
- Disaster definition
- Critical applications
- Organization policy on DLE
- List of departments, major functions with process owner(s)
- DLE impact by business function



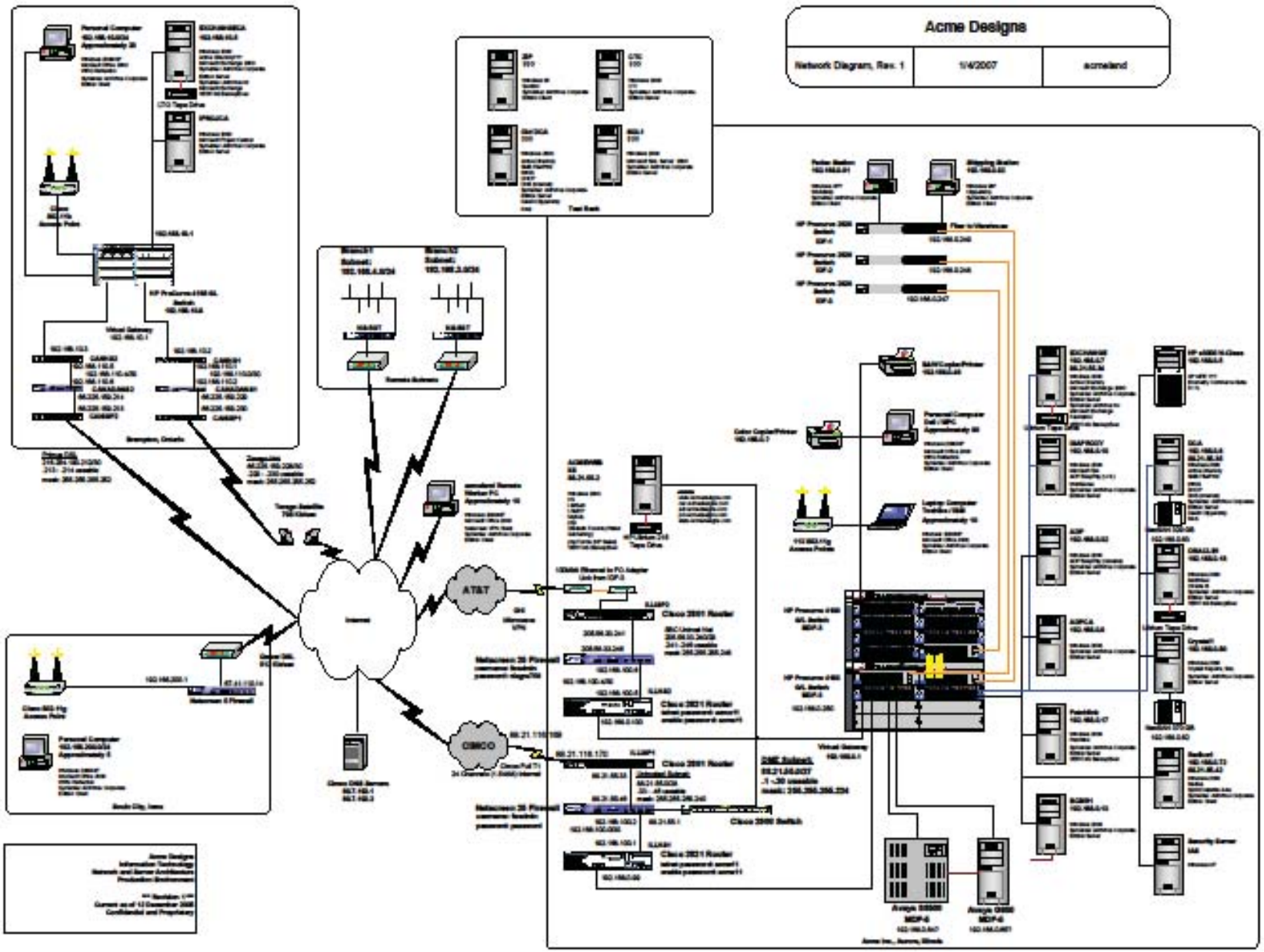
Team and Contacts

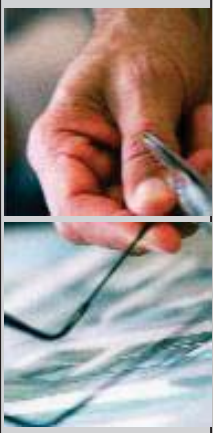
- DR team and responsibilities
- Contact information for process owners and IT staff (home, work, cell)
- Vendor information
- Off-site storage information
- Information about alternate site if applicable



Current Environment

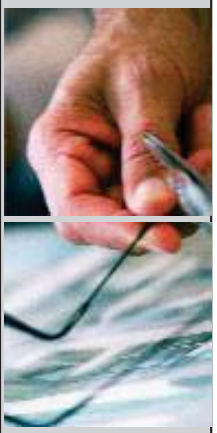
- Network diagram
  - Include IP address information
  - Purpose of servers
  - Firewalls
  - Other
- System hardware and software
  - Mainly limited to servers
  - Backup and restore procedures
  - Administrative password policy
    - Identify what hardware has passwords (servers, routers, firewall, other)


Acme Designs
Network Diagram, Rev. 1
1/4/2007
acmeland
AT&T
CISCO
Internet
Cisco 2801 Router
Cisco 2821 Router
Cisco 3560 Switch
Avaya S8500
MDF-0
Avaya G650
MDF-0



Disaster Implementation Tasks

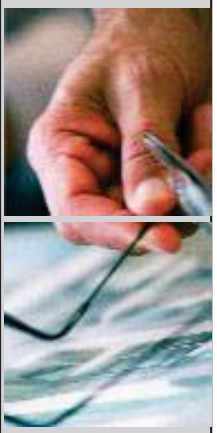
- Who declares a Disaster has happened
  - When do you start using the plan?
- Recovery procedures
- If appropriate, alternate site information
- What the recovery environment will look like
- Procedures to use alternate site
- Who to contact, backup to main contact



Test the Plan

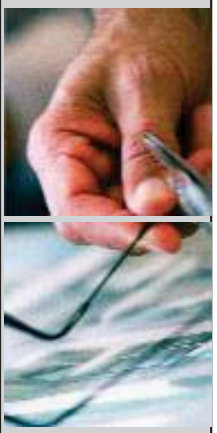
- Describes how you will test the plan
- How often you will test, review
- Without testing your planning is NOT complete

Sikich



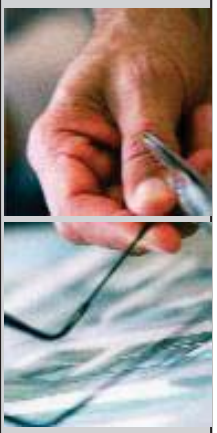
Recovery Plan Maintenance

- How to maintain the plan
  - Periodic reviews
    - Changes in organizational processes
    - Change in remote locations
    - Change in the network environment
  - Where the documentation is stored



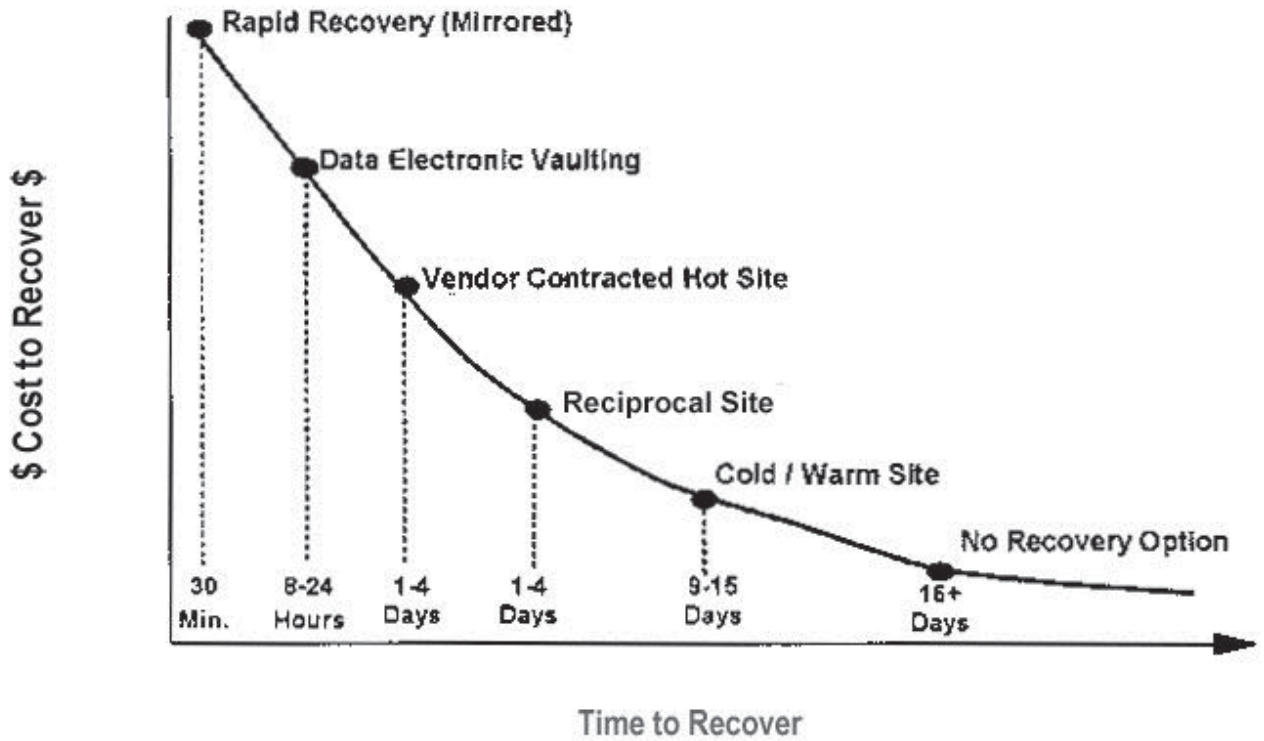
Test the Plan

- You did all this planning, does it work?
- Testing will uncover flaws and oversights
- Testing will give you peace of mind
- Periodically (once or twice a year) test the plan as your organization will continually change:
  - Staff who wrote the original plan are gone
  - Locations
  - Applications
  - Processes
  - Size
  - Changing regulations

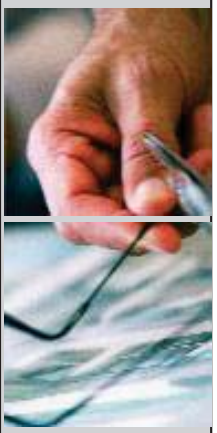


Solutions and Other Considerations

Cost to Recover Vs Time to Recover

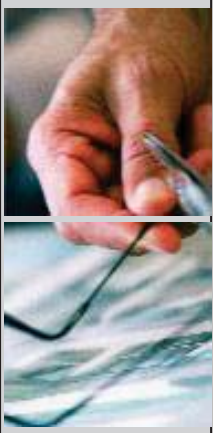


Sikich®



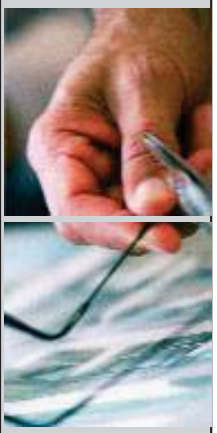
What About E-mail?

- How would your organization react without email for a day, a week?
- E-mail for many is mission critical
- E-mail issues for DR Planning:
  - Retention of email – legal
  - Many organizations store important information in emails and use as an information data store, thus backups can be critical
  - Ability to receive email when server and/or connection is down
- Consider an IM solution as a backup



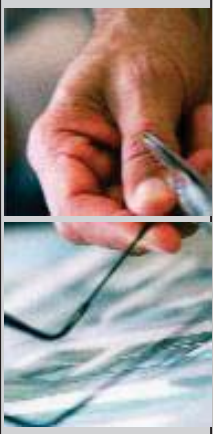
Keeping the E-mail Going

- Many ISP's offer "mail bagging"
  - When email can't get through to your server they save it for you
- If you have multiple Exchange servers you can have one act as backup to the other



Don’t Forget…

- Desktop and laptop data
  - Presents a backup problem – address it
  - All documents that are required to run the organization need to have a copy on network drives
  - Enforceable by company policy/rules
  - There is technology that can backup laptops when connected to the network
    - eVaulting (online backup and recovery)
    - Software



QUESTIONS?

Presented by:
Scott Wegner
Partner, Director Networking Services
Sikich LLP
1415 W. Diehl Road, Suite 400
Naperville, IL 60563
(630) 566-8417
swegner@sikich.com

©2012 Sikich LLP. All Rights Reserved.