10/18

Just another day at the office?

If you recall…

9/11

started out the same way.

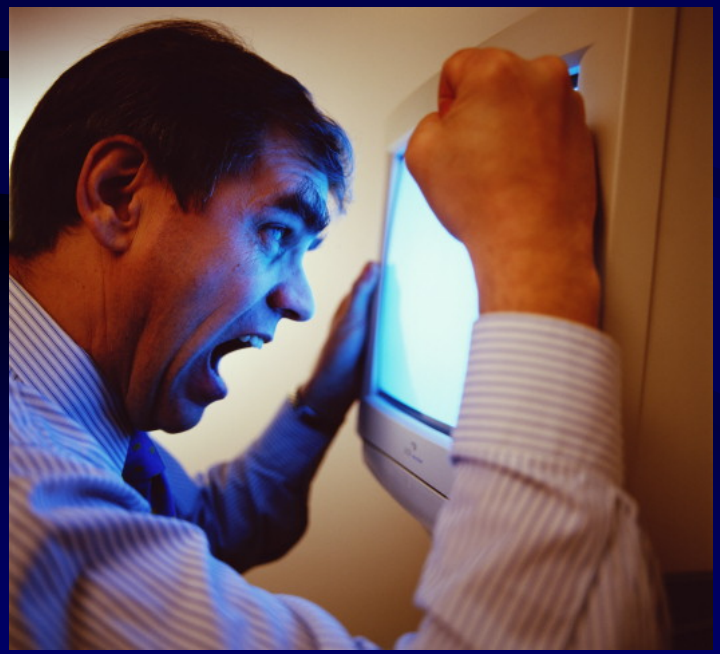
Disaster Recovery
vs.
Operational Assurance

Getting the Most Protection With a Limited IT Budget

Christopher Furey – CEO Savvy Networks

Disaster Recovery Planning is a Very Stressful Process.

It Carries a Stress Level
That is Only Surpassed by
Experiencing An Actual Disaster
From Which You Must Recover



Bad things happen to good people,

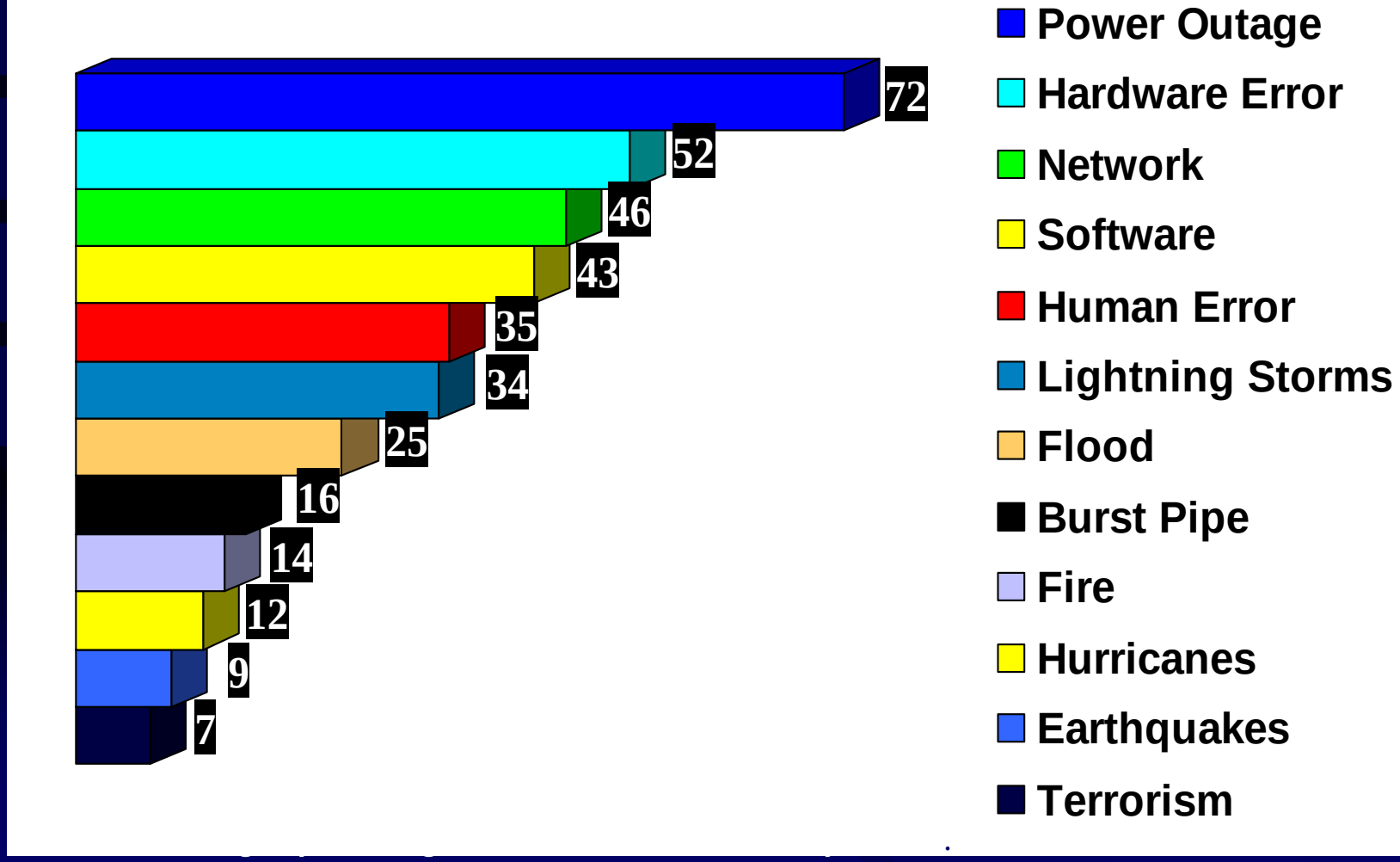
but successful people prepare for the worst.

Topics of Discussion

- What qualifies as a disaster?
- What is disaster recovery (DR)?
- Typical approaches to DR
- What is Operational Assurance (OA)?
- Typical approaches to OA planning
- Summary

What is a disaster?

Disasters Happen Locally and Regionally



Luck – Don’t Count On It

Luck - bad and good - will always be with us. But it has a way of favoring the intelligent and showing its back to the stupid .

- John Dewey

Shallow people believe in luck and circumstances. Strong people believe in cause and effect.

- Ralph Waldo Emerson

Understanding IT Risk – What is the Business Impact?

- 75% of all US firms have suffered a severe business interruption.
- 43% of US companies never reopen after a disaster and 29% more close within three years.
- 1 in 5 small to mid-sized firms suffer a major disaster every 5 years
- Viruses, Spyware & Malware are more prevalent, costly, destructive and caused more real damage to data and systems last year than ever before. Network virus attacks average 21 hours of downtime to properly clean PCs and servers.
  (Source: 9th Annual ICSA Lab's Virus Prevalence Survey - March 2004.)
- Organizations that aren't able to resume operations within ten days (of a disaster hit) are not likely to survive.
  (Source: Strategic Research Institute, Jan. 2002.)

Plan For Survival

Dramatic change often comes as a response to imminent collapse.

- Tom Peters

Strategy is not the result of planning, it's the place where planning begins.

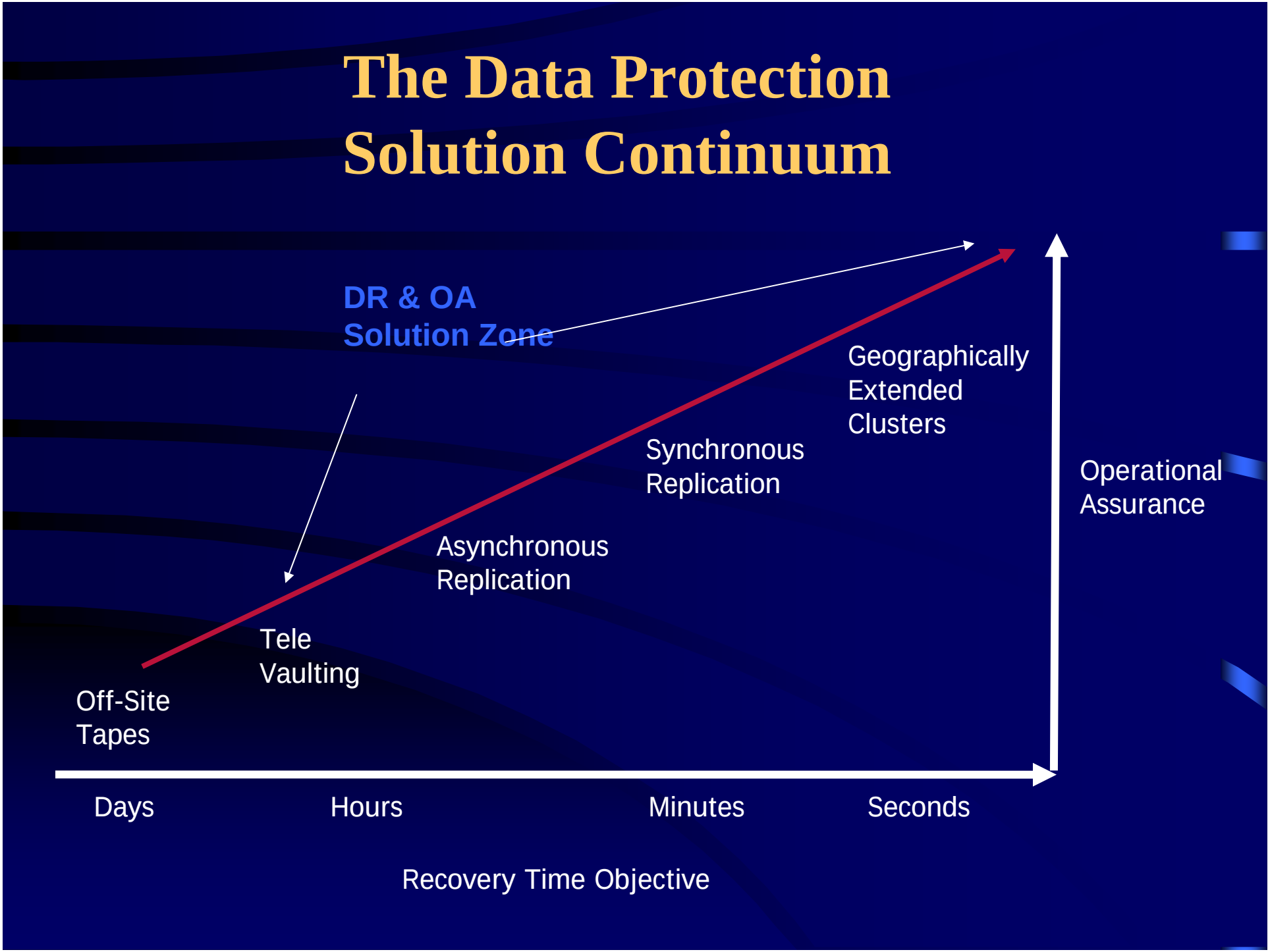
What is Disaster Recovery?

- Typical answer – DR is IT **system recovery**
  - What systems?
  - Recovered back to when?
  - Isn't that why we have backups?
- A better answer is: *disaster recovery is the planned and coordinated process of restoring systems, data and infrastructure required to support ongoing business operations.*

Understanding IT Terms Used

- “Systems” include both hardware & software
- “Data” includes actual data files, logs and audit information, as well as “business knowledge” (procedures and business rules)
- “Infrastructure” includes phones, people space, RAS systems, intranets, websites, firewalls
- “Business operations” are the things your organization does each day to generate revenue

The Data Protection Solution Continuum



Typical Best Approach to DR

- The Hot Site
  - Need to maintain redundant facilities
  - Use of storage area networks (SAN's) is ideal from a technical perspective
  - Real-time data replication or restore from current backups are two commonly used techniques
  - Hot sites generally provide the benefits of proximity and availability
  - Require sufficient bandwidth for daily data transfer
  - A true "hot site" is usually the most expensive, fastest to recover and most reliable approach to DR

Typical Approaches to DR

- Use DR Facilities and Service Providers
  - Cost is “fixed” over the life of the contract
  - There are usually extra costs for testing
  - Contracts may lack absolute guarantees and/or service level agreements (SLAs)
  - Hardware configuration issues are common
  - Availability issues may occur
  - Possible bandwidth or accessibility issues
  - Is your provider committed to your success?

Typical Thinking on DR

- "We will just restore from our backups"
  - Where will the restore physically occur?
  - Are you certain your backups are current?
  - Are you sure your backups are good and will restore?
  - Will the disparate systems data be in sync?
  - What about offsite backups that may be older?
  - Is the replacement equipment compatible?
  - What is your best case recovery time?
  - What about access, bandwidth & network security?
  - What about "*running the business*"?

Some Truths About DR

- Even with planning, DR is REACTIVE at best
  - Cost is often over $1000 per month per server
  - Duplicate software licenses are required
  - Contingency people space costs >$150/seat/mo
  - Facilities are not guaranteed to be available
  - Periodic testing can cost over $25,000 per year
  - Staff tends to go home to “nest” in a disaster
  - Successful “on-time” recovery cannot be assumed
  - Management usually lacks subject matter expertise and/or a strong advocate at senior level

Reinforcing IT Infrastructure - Protecting the Crown Jewels

IT is a Performing Business Asset
& Delivers Important & Strategic Competitive Advantages

IT Infrastructure Processes and Stores Confidential Business Information:

Financial Data, Customer Lists, Supplier Contracts, Manufacturing Schedules, Engineering Designs, Patent Information, Trade Secrets, Human Resources Records, Business Plans, **Email & Groupware**

Information is a vital and valuable corporate asset which is vulnerable to mismanagement and abuse. Stakeholders deserve protection.

To be effective, IT Must Be Constantly Managed & Protected.
Take your information for granted at your own risk!

Definition of Operational Assurance™

(op·er·a·tion·al as·sur·ance) - *n.*

1. the management practice committed to maximizing business productivity by increasing IT systems uptime;

2. the discipline of protecting and keeping available an organization's intellectual capital;

3. a proactive, cost-effective process which ensures resilient, predictable, compliant and secure IT infrastructure.

The Difference Between DR and Operational Assurance

- DR is REACTIVE – OA is PROACTIVE
  - DR is hard to fund because management often feels disasters are so rare that decisive action is deferred
  - OA brings real-time benefits to the organization
  - OA is “applied best practices” in IT management
  - A properly staffed and funded IT effort considers and addresses the holistic needs of the business.
  - OA is to well being - what DR is to disease mgmt
  - Living well keeps you healthy & stronger longer

OA is Smarter Than DR

- Fixes the small stuff that can become big stuff
  - Ensures that power is adequately supplied to IT
  - Remedies environmental infrastructure issues
  - Builds in redundancies & resilience for core services
  - Assures professional handling of data protection
  - Provides accountability to management
  - Plans beneficial outcome into continuity planning
  - Delivers measurable value to stakeholders
  - Helps protect the organization against loss

Where to Start?

- Create an OA or IT Continuance team
  - Executive sponsor is a must
  - OA coordinator (internal or outsourced)
  - Team leader and members
  - Need to define both primary and backup contacts for each team position. The goal is to avoid having any one person become a “single point of failure” in the plan.

Where to Start?

- Prepare an accurate audit of your network
  - Inventory all hardware (models & serial numbers)
  - Inventory all essential software (version numbers)
  - Document all software licenses and key codes
  - Collect and properly file all software masters
  - Document all vendors & key external contacts
  - Identify weak links and single points of failure
  - Tie off all hardware & software to departmental and core business functions and managers

Where to Start?

- Identify your business requirements
  - Requirements are different than goals!
  - Identify functional areas to be covered (for example: locations, lines of business, specific unit or departmental functionality)
  - Categorize those items into priority 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 Recovery Time Objective (RTO) This is the target goal for having essential systems back in operation.
  - Define Recovery Point Objective (RPO) This is how much data can be lost based on the time of the failure moving backwards to your last known good total backup
  - Set expectations based on this common understanding of the business goals

Where to Start?

- Identify and categorize risk
  - What is most likely to occur
    - Fire? – Our area's most likely cause
    - Natural disasters (flood, hurricane, tornado, earthquake)
    - Loss of infrastructure (power, phones, internet, facilities)
    - Hackers, viruses, worms, terrorists, misc. evil
  - Look at the probability and the cost of each type of disaster event, 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 (HIPAA, SarbOx, GLBA, FDA, DoD, NASD, etc.) **If so, you need to ensure compliance on an ongoing basis!**

Where to Start?

- Identify Key Personnel
  - They may not be part of the OA Team!
  - They often include outside contractors!
  - Identify Roles and Responsibilities
  - Associate Names with Roles
  - Have a clear and secure policy defining who has authority over what and when
    - For example, what constitutes a disaster, who can declare a disaster and under what circumstances.

Typical OA Continuance 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 screen output from those commands
  - Provide check boxes and an area to write in time started/time completed and comments
  - Cross-training provides both depth of coverage and validation of the process

Typical OA Continuance Plan

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

When to Start?

- Get started today or empower someone else now!
  - All OA plans require a commitment to proceed
  - Most organizations think someone else has already done the planning already
  - Good intentions don’t save the day
  - A proactive OA approach is less costly and more efficient than a reactive DR approach
  - Find a subject expert to advise and consult

QUESTIONS?

- Ideas to share
- What's working for you?
- What obstacles need to be overcome in your organization to ensure proper planning?