

NTEN 2007

Disaster Preparedness Today

Tony Dempsey

Manager of Information Technology
American Association of Colleges of Nursing

Tim Johnston

Chief Technology Officer
NPower Greater DC Region

MD Huda

Senior Director of MIS
Mary's Center for Maternal and Child Care



Session Outline

1. Meet the panelists
2. What's it all about?
3. The Basics: keeping it simple
4. Getting buy-in
5. Some practical, tactical tips
6. Panel Discussion: Preparation Best Practices
7. Panel Discussion: Recovery Best Practices
8. Your questions



ONE

MEET THE PANELISTS



Meet the Panelists

◆ Tony Dempsey

- Manager of Information Technology, American Association of Colleges of Nursing
- Graduated with a BA in Economics from Newcastle Polytechnic, Newcastle, England; in the USA for 24 years
- MCSE certified, 11 years IT experience in both support & management roles; 9 years in non-profit environment
- Experience includes network administration, end-user support, database design, application design, business continuity planning, end-user training
- Previously worked for Signal Corp. on government contracts; journalist at USAToday



Meet the Panelists

◆ MD Huda

- Senior Director of MIS, Mary's Center for Maternal and Child Health
- Graduated of Bangladesh University of Engineering & Technology
- MCSE, trained as CCNA & CSPFA, CISSP candidate
- 20 years experience in various IT environment including Hardware, Software, Architecture, Computer aided design, Security, EMR, HIPAA, Management, Planning & Implementation
- Worked in USA, Singapore & Bangladesh
- 7 years of non-profit experience; 4 years in IT management



Meet the Panelists

◆ Tim Johnston

- Chief Technology Officer, NPower Greater DC Region
- BA Psychology from Duke University; MBA and MS in MIS from Boston University
- 20 years IT experience
- Database development, IT management, business continuity, web development and marketing, non-profit management
- CIO at \$130MM non-profit, Business/Marketing for non-profit online medical courseware developer, database consulting business, Executive director of a non-profit



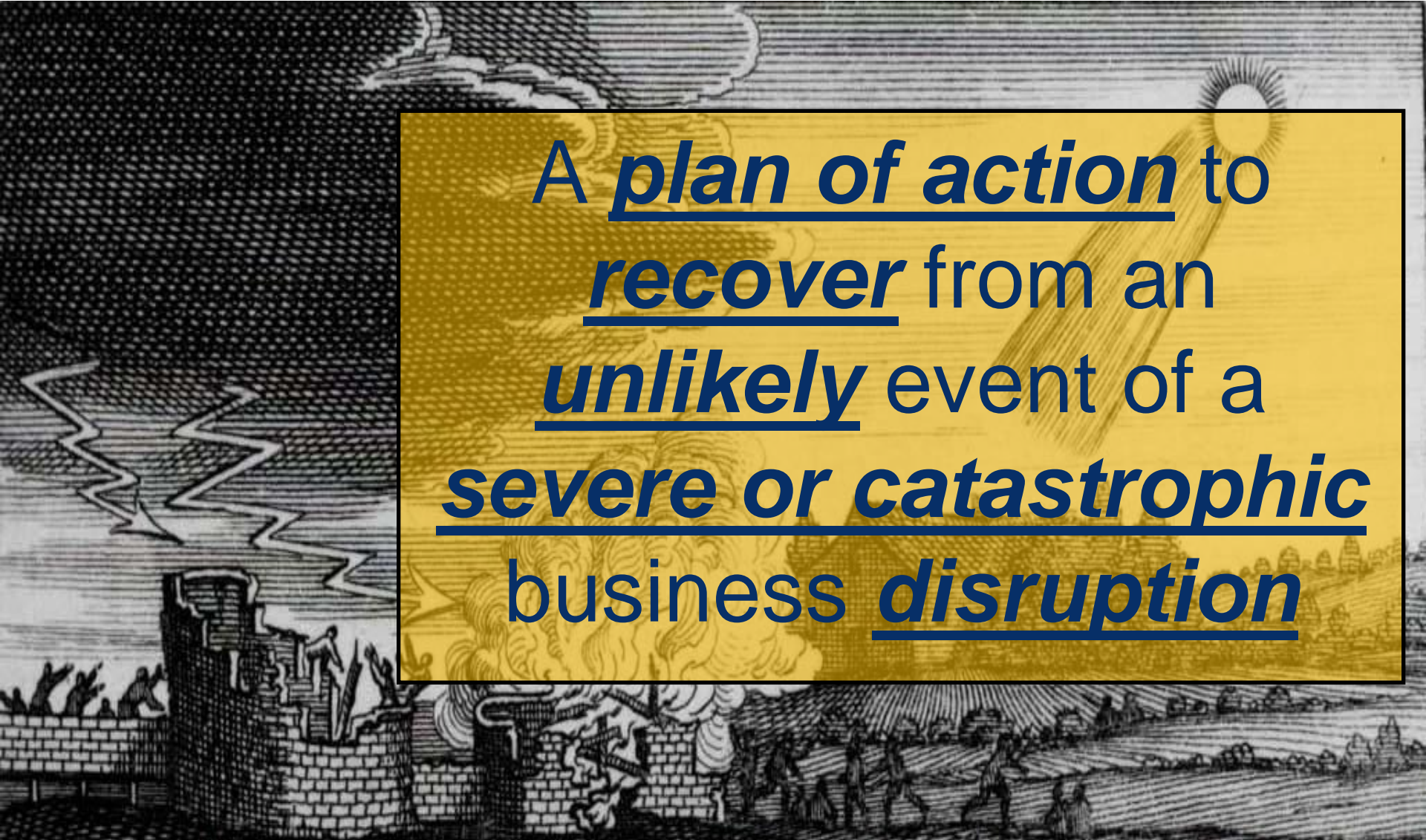
TWO

WHAT'S IT ALL ABOUT?



What's it all About?

What is a Disaster Recovery Plan?



A plan of action to recover from an unlikely event of a severe or catastrophic business disruption

What's it all About?

Some Terms

◆ Disaster Planning

- How do you prepare for a disaster, reduce risk, impact

◆ Business Continuity

- What's involved in keeping the business running
- How to ensure processes continue despite a loss of infrastructure

◆ Disaster Plan

- Usually, what we're going to do and who's going to do it
- **May** be broad enough to answer the continuity question, but that's frequently missing



What's it all About?

The Worst Case Scenario

No Plan



What's it all About?

The Basic Truths

- ◆ Disaster Recovery is not an IT issue; you should own the IT part
- ◆ Today's business and system complexity makes identifying and quantifying risk more daunting than ever before
- ◆ Before you can manage risk, you must identify it and quantify it
- ◆ Appropriate response is defined differently for each organization
- ◆ You can decide to do nothing*
 - * important caveats follow
- ◆ Planning is evolutionary and ongoing



What's it all About?

The Basic Truths

The Planning Process



What's it all About?

The Basic Truths

- ◆ Today's fast and competitive business environment
- ◆ And system complexity
- ◆ Make identifying and quantifying risk more daunting than ever before



Disaster Recovery: Then and Now

Then:

- Move operations to the curb
- Local customers, suppliers, communication expectations
- Find another DEC PDP11 at the market

Now:

- Wider spheres of influence and communication
- More stakeholders with different communication expectations
- More competition/substitutes
- Much faster cycle times



Before you can
manage risk,
you must
identify and *quantify* it



Identifying and Quantifying Risk

- Risk Factors: What does it look like?
 - Probability—High, Medium, Low
 - Speed of onset—Sudden, Gradual
 - Forewarning—Yes, No
 - Duration—Long, Short, Indeterminate
- Risk Impact: What can it do?
 - Financial—what's the cost to fix? What's the loss of revenue?
 - Operational—how does it affect operations?
 - Human—what's the impact on staff, clients, other stakeholders?
 - Reputation—how would this affect your reputation (funding, clients)
- Risk Mitigation: What are the options for avoiding it?
 - Cost—What can you **afford** to do?
 - Degree—What do you **want** to do?



What to Plan for?!

◆ YES

- Server/Equipment failure
- Power/Internet outage
- Fire

◆ ?

- Avian flu
- Nuclear holocaust
- Hostile takeover
- ...



Appropriate response
is
defined ***differently***
for each organization



THREE

THE BASICS



Plan Elements

◆ The Business Impact Analysis

- **Identifies** the threats to your people, processes, and technology
- **Quantifies** potential damage of interruption by threats

◆ The Disaster Recovery Plan

- Spells out the why, what (and what NOT,) who, where, when, and how;
- Of your intended (appropriate) responses to identified risks;
- Given your organizational ability to avoid these risks
- And your collective tolerance for risk.



It's the Continuum, Stupid

You can decide to do *nothing*...but plan for that in writing.



What's Reasonable?



Unreasonable:

- No written plan

Reasonable:

- Conduct a Business Impact Analysis for each department, process, or core function
- Identify what you will and will not do. You can decide to do nothing for some processes—but document that decision
- Fit the plan to match organizational and individual risk preferences
- Modify, grow, adapt as systems, processes, stakeholders, and risks change

FOUR

GETTING BUY-IN



ONE

◆ Start at the top

- If executives aren't on board, it's going nowhere
- If not the ED, how about the Board of Directors?

◆ Start in the middle

- Work with key process owners to help them understand risk and recovery times
- Have them express concerns to ED



- ◆ Use the Business Impact Analysis
 - Push responsibility to the department or process level
 - When process owners quantify the impact, they begin to take responsibility



Getting Buy-in

THREE

- ◆ Conduct a “Table Top” disaster drill
 - Gather department leaders in a room
 - Spring a scenario on them
 - Ask everyone how they’d respond and keep the work going
 - This process surfaces all kinds of misconceptions and incorrect assumptions!
 - “You mean we don’t have a backup email system?”
 - “I thought that was IT’s job!”



- ◆ Seek funding for disaster planning and infrastructure
 - If you have access to funders
 - Explain the impact of various scenarios
 - Explain the cost of mitigating the risk



- ◆ Ensure that executives and managers understand what data backup provides
 - Data backup is not application backup
 - May take **days** to restore functional use of the backed-up data!



- ◆ Repeat again and again, “business continuity is a business issue, not an IT issue.”



FIVE

PRACTICAL, TACTICAL TIPS



FIVE

PRACTICAL, TACTICAL TIPS



ONE

- ◆ Have good antivirus protection and data backups
 - Most common issue!
 - Take backups offsite
 - Use managed antivirus clients (Symantec Corporate Edition from TechSoup)



TWO

- ◆ Identify all single points of failure
 - Where might a little redundancy go a long way?
 - Are you dependent on others—space, shared connectivity, etc.?



THREE

- ◆ Keep critical info on a USB Key
 - Phone numbers of all staff and vendors, passwords, etc.
 - Copy of disaster/continuity plan!



FOUR

- ◆ Post a contact sheet on building door
 - Tell stakeholders how to find you



FIVE

- ◆ Have an alternative means of communication
 - Home phone, cell phone, place to meet (virtual or real), conf call service
 - Consider an externally hosted intranet
 - Almost free these days



- ◆ **Have a staff backup person**
 - Who can fill in for you if you're unreachable?
 - Return the "favor"



SEVEN

- ◆ Have an external backup person
 - Who can you turn to for extra help when you need it?
 - Trusted vendor(s), IT at other nonprofit



EIGHT

◆ Off-site storage

- Online backup is relatively cheap, IF you manage your data
- Keep copies of application software offsite
- Have a reciprocal agreement with another non-profit to store key stuff



NINE

- ◆ Be aware, be very aware
 - Weather, power issues, (computer) virus alerts



- ◆ Take baby steps and iterate!
 - Perfection is the enemy of good
 - Use “unfortunate events” to improve the plan
 - Use new business risks to improve the plan



Additional Takeaways

- ◆ We'll post some additional materials on the NTEN site
 - Business Impact Analysis Template
 - Sample disaster plan
 - NPower Guide to Business Continuity



SIX

PANEL DISCUSSION: PREPARATION BEST PRACTICES



SEVEN

PANEL DISCUSSION: RECOVERY BEST PRACTICES



EIGHT

YOUR QUESTIONS



Thank you!

