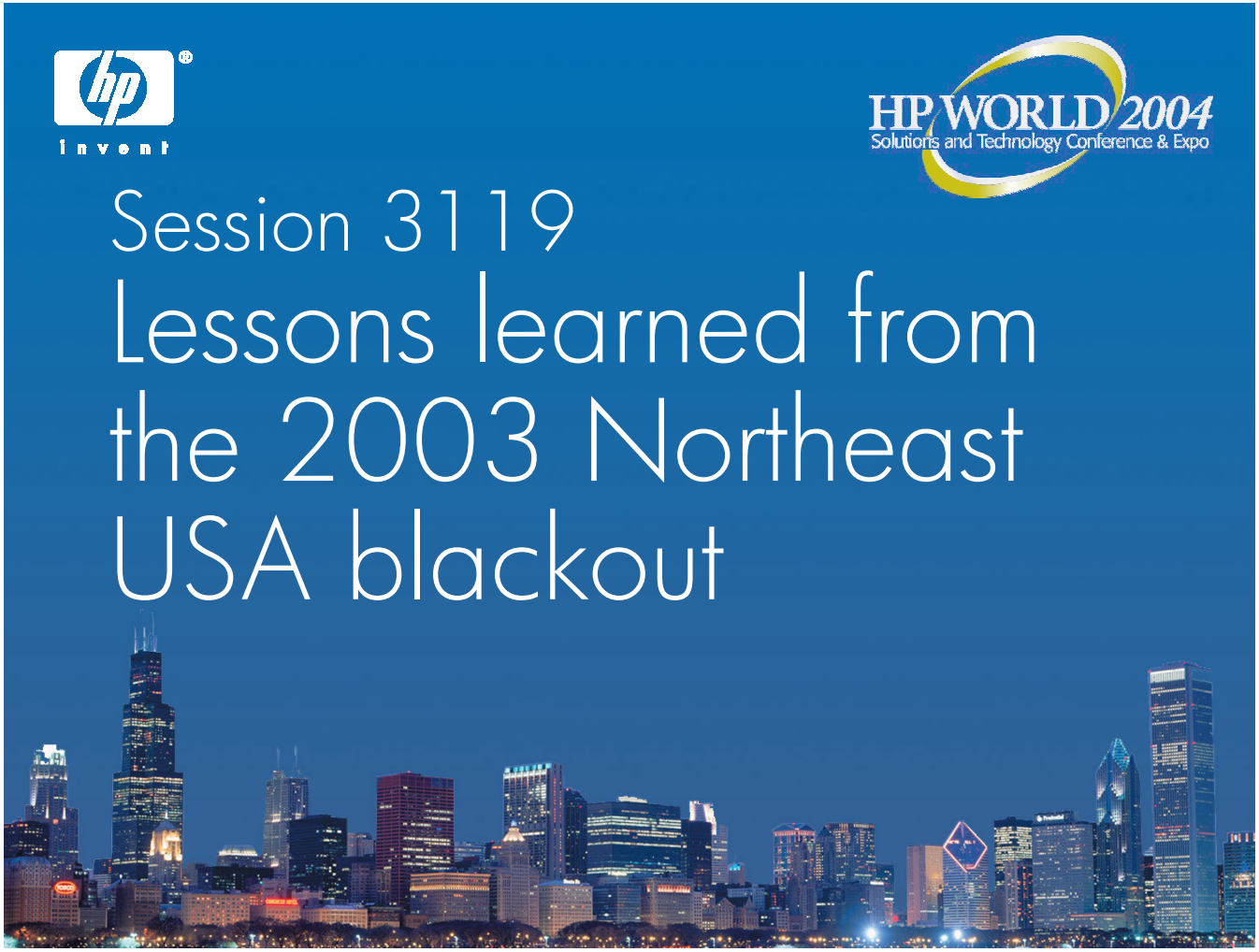


HP WORLD 2004
Solutions and Technology Conference & Expo

Session 3119

Lessons learned from the 2003 Northeast USA blackout

Ron LaPedis, CBCP, CISSP, ISSAP, N6QGK
Sr. product manager, NonStop Division

Agenda

- What happened
- What *really* happened
- We are more dependent than we think
- What did and did not work
- Airports, hotels, and so on
- Lessons learned
- What you can do for your family
- What you can do for your company

The 2003 Northeastern Blackout -- What happened

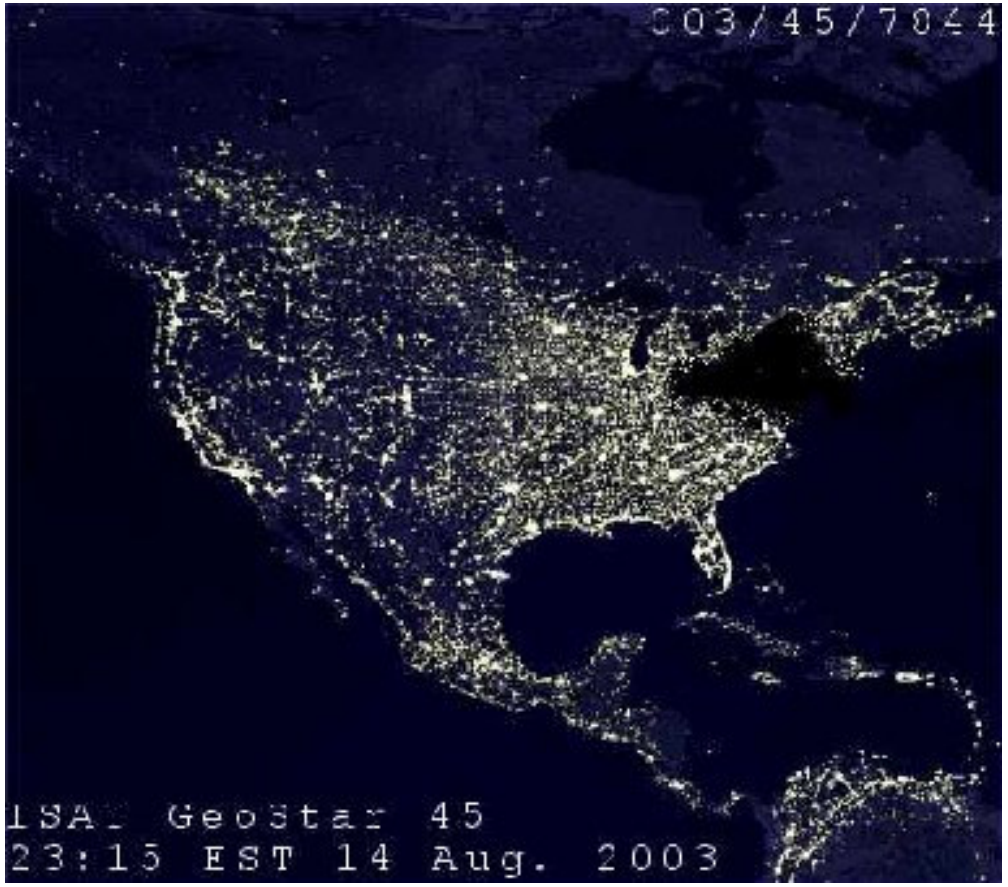
- Major outage (93,000 square miles, 60 million people) was from 16:10 Thursday August 14 to 21:03 Friday August 15.

- Thousands slept in subways, under their desks, or under the stars

The 2003 Northeastern Blackout

It's a hoax

- There is no imaging satellite named "GeoStar."
- The timestamp shows "23:15 EST," but satellite images are usually marked "UT" (Universal Time) — and the U.S. is currently on Daylight Savings Time.



Source: http://urbanlegends.about.com/library/bl_blackout_photo.htm

The 2003 Northeastern Blackout -- The real picture

- Community power plants, batteries, generators, and UPS meant that not everyone in the area was affected as seen by the lights still on.

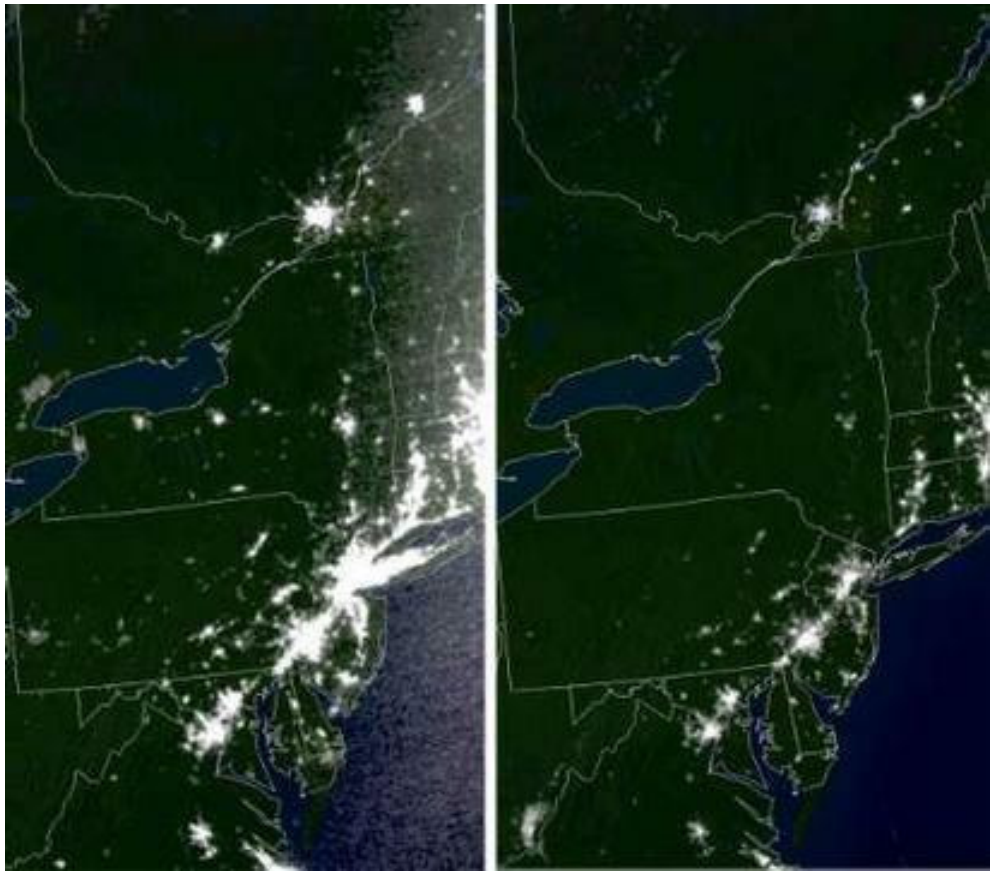


Photo: NOAA/ Defense Meteorological Satellite Program

What *really* happened

- Three of the FirstEnergy's high voltage lines in Ohio sagged into unkempt trees and "tripped" off.
- Because FirstEnergy's computerized alarm failed silently, control room operators didn't know they were relying on outdated information.
- Trusting their systems, they even discounted phone calls from other energy suppliers warning them about worsening conditions on their grid. After all, the alert systems were not reporting any alerts.

Source: http://www.theregister.co.uk/2004/04/08/blackout_bug_report/

Multiple failures

- After the alarm function crashed in FirstEnergy's control center, unprocessed events began to queue up, and within 30 minutes the EMS server hosting the alarm process folded under the burden.
- A backup server kicked-in, but it also failed.
- By the time FirstEnergy operators figured out what was going on and restarted the necessary systems, hours had passed, and it was too late.

Tracking down the cause of the crash

- One-million lines of code comprise the General Electric A/21 Alarm and Event Processing Routine, written in the C and C++ languages.

- About eight weeks after the blackout, GE was able to reproduce the Ohio alarm crash in GE Energy's Florida laboratory.

The results

- GE had to slow down the system, injecting deliberate delays in the code while feeding alarm inputs to the program.

- The bug was unmasked as a particularly subtle incarnation of a common programming error called a "race condition," triggered on August 14th by a perfect storm of events and alarm conditions on the equipment being monitoring. The bug had a window of opportunity measured in milliseconds.

Design flaws

While the bug was subtle, there were other design flaws:

- The alarm system failed silently
  - The operators did not know that it had failed and was displaying stale data.
- The alarm queues backed up causing that host to fail
  - Bad design that does not handle queue overflows.
- The backup alarm queue processor kicked in and quickly failed
  - Bad design of an allegedly high-availability system

Not an isolated case

Hardware and software can fail, even HA systems.

It is every company's duty to ensure:

- Failures are not silent but will be detected
- There are procedures to deal with failures
- Your employees know where to locate the procedures
- The procedures are exercised regularly
- The procedures are updated regularly


We are more
dependent than we
think

We are more dependent than we think

- Following any disaster, phone lines and cellular towers may be damaged, overwhelmed with volume, or set to ignore all but high priority calls, making it difficult to get calls through to an area.

- Reports from those on the ground state that Nextel Direct Connect® continued to work

We are more dependent than we think

- Electronic flush toilets
- Electric eye water faucets
- Card key systems
- No drinking water due to pump failures (1 million persons)
- Mobile phone cell sites down because no backup power
- Cordless phones, voice over IP

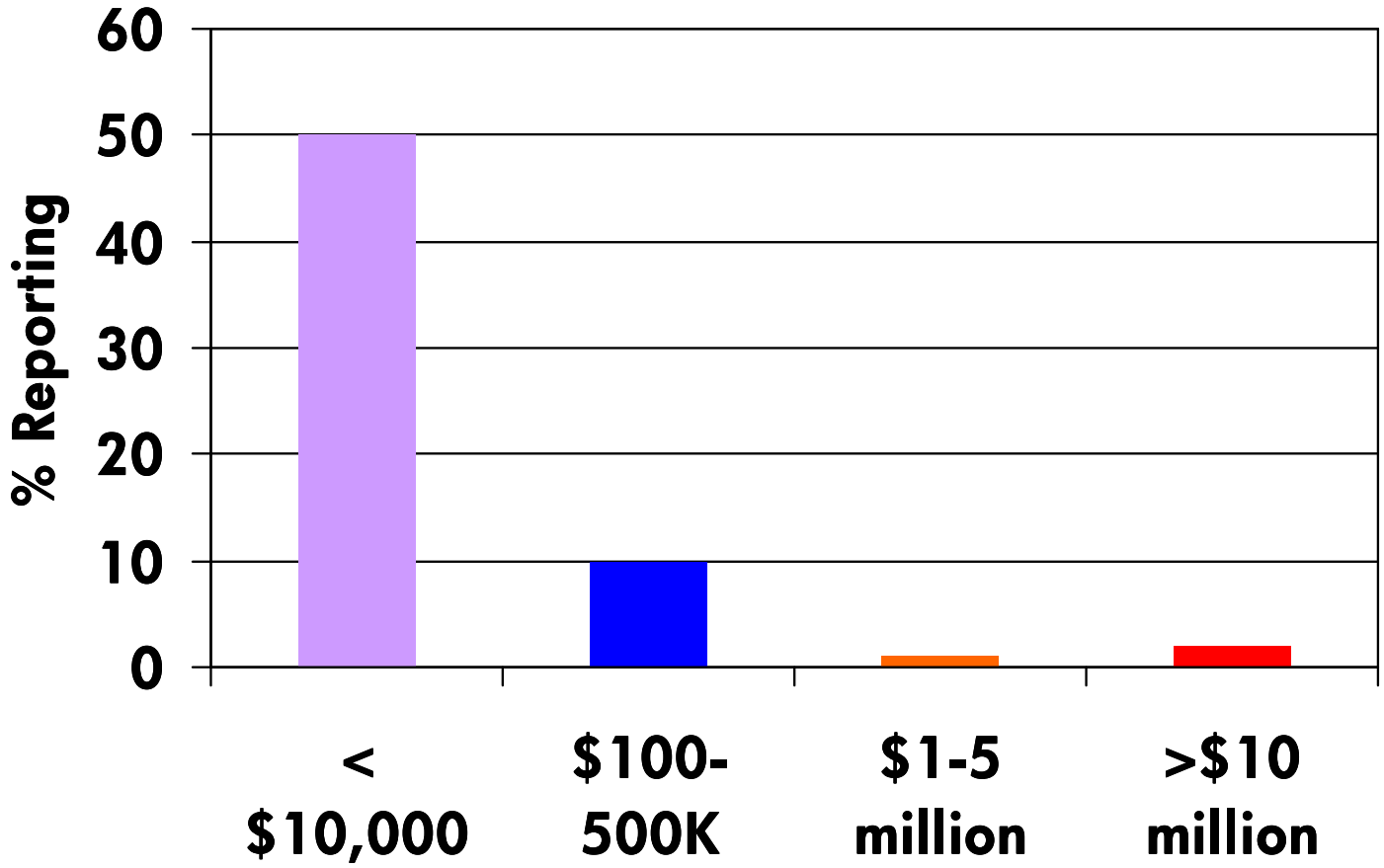
Source: CNN

We are more dependent than we think

- Air conditioning (temperature was 92F, 33C), and many high rise windows do not open.
- Subways, electric trolleys/streetcars
- No water, escalators, elevators, fire alarms, or sprinklers in tall buildings.
  - Unless on backup power
- 800 elevator rescues, 80,000 calls to emergency services

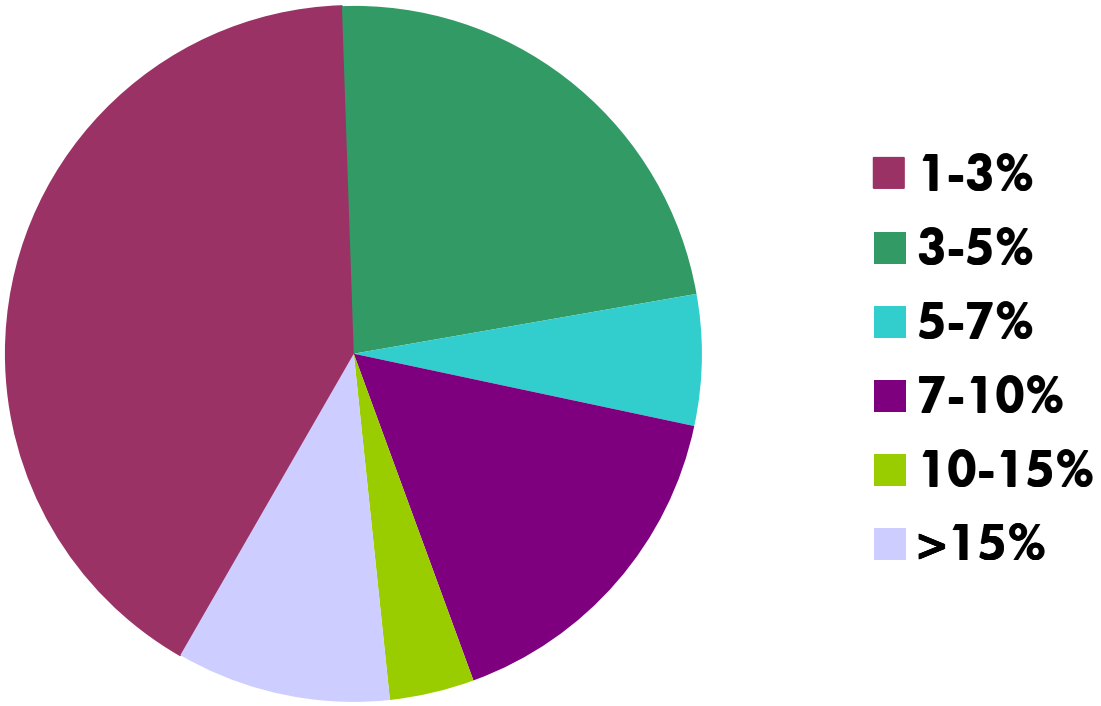
Source: CNN

Productivity loss from the blackout



Source: AFCOM survey

Planned increase in DR spending – After the horse has left the barn…



Source: AFCOM survey

This is not rocket science

- You power up the generators and nothing happens.
- You power up the generators and the power surge blows out your systems.
- You power up the generators and realize that your air conditioning isn't on backup power.

Hint: exercise your plan

There were problems

- Companies had backup sites located in the same outage zone.
- NYSE ran on generators overnight until regaining power on Friday at 06:00.
- American Stock Exchange had backup power to systems but not to cooling. Opened 15 minutes before closing time on Friday to exercise expiring options.

Source: Wall Street Journal

But many plans did work

- AOL's modem banks, which relay data over phone lines in New York City and Detroit and other affected regions, had gone down after local electricity grids blinked off Thursday evening.
- More than fifty AOL engineers and technicians raced around the clock to ensure AOL's 25.3 million members in the United States and many Canadian members were not unplugged by the incident.
- Some subscribers living in blackout areas who were desperate to check e-mail or keep abreast of any late-breaking news chose instead to dial access numbers in other cities not affected by the event.

Source: Reuters

Hot site vendors came to the rescue

- 34 SunGard customers called to activate their disaster plans, and an additional 100 put SunGard on notice.

- HP was able to seamlessly transition 14 customers supported by dual data centers in Toronto to battery-operated Uninterruptible Power Supplies, then to backup diesel generators loaded with enough capacity for one full week.

Source: Reuters

We always fight the last war

- Before '93 WTC bombing, backup site in same tower.
- Before 9/11, backup site in the other tower.
- Before 2003 blackout, backup sites in the same city or outage area.
- What's next?

Source: Wall Street Journal

The government took action

- Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System
- On September 5, 2002, the agencies published for comment a draft of the paper in the Federal Register.
- On April 8, 2003 the final version was released to the public.

http://www.sec.gov/news/studies/34-47638.htm

Source: Wall Street Journal

…which was resisted

- "The final paper, …provides more flexibility to firms in managing geographic dispersion of backup facilities and staffing arrangements, and takes into account other considerations relevant to cost-effective implementation of sound practices."

http://www.sec.gov/news/studies/34-47638.htm

Source: Wall Street Journal

Do you remember how to start your HA system?

- One HP NonStop customer had an operational issue when power was restored. Apparently they were not familiar with how to start their system, applications, and terminals. The GCSC assisted the customer with coldloading the system.

Airports

- Airports shut down in New York, Detroit, Buffalo, Cleveland, Toledo, Toronto and Ottawa, among others. Some operational Thu PM.
  - While air traffic control centers and many airports had backup power for some areas, operations were shut down because the outage crippled security screening facilities, bag handling, reservations and other airline operations.

- One industry expert said the cost to the airlines' bottom lines is likely to reach into the tens of millions of dollars once the dust settles, not a huge amount for the industry, but not a help considering the ongoing losses at many airlines.

Source: CNN & Reuters

Hotels

- Room cardkeys – doors are battery operated, but the staff couldn't make new cards
- Backup generators at the 1,946 room Marriott Marquis NYC failed, despite being tested weekly and serviced 3 weeks before. This left the hotel without water, elevators, fire alarms, or sprinklers. Guests had to be evacuated and slept under the stars. Staff with flashlights climbed 47 flights of stairs to retrieve prescription medicines and other guest items.

Source: USA Today

Lessons learned

Exercise your plan

Lessons Learned

- Spreading backup systems around geographically for security/continuity purposes needs to be done across hundreds if not thousands of miles. Building a backup facility across the street or across the river just doesn't cut it. Companies will need to rethink what it means to create truly redundant business operations.
- While security analysts have painted a fearful picture of what would happen if terrorists combined a major attack with a well-timed and well-executed cyber-assault, a similarly nasty one-two may be just as likely to occur without any terrorist (or human) intervention at all.

Lessons Learned

- Know your recovery requirements and the risks you face.
- Ensure you have enough backup power and all critical components are connected to it.
- Cordless phones & VOIP fail when the power fails.
- If your plan requires employees to travel by air to a backup site, do you have an alternate travel plan?
- You may not be able to rely on mobile (cellular) phones in a disaster. If your plan relies on them, consider changing it now.
  - Amateur radio operators can help with people and property safety. Start a club at work (HP has one). www.arrl.org

Lessons Learned

- Electronic doo-dads may be nice…
  - but only if they are working (toilets, faucets, etc.)
  - Check out your company when you get home -- would you need to evacuate your office for safety reasons?
- Have emergency food and water for 3 days on hand.
  - Should your company have a program to offer employee discounts on bundled emergency kits?

Lessons Learned

- Safe haven for employees and perhaps one or two relatives.
- Talk to landlords about their building policies.
- Location of offices, crisis room, and living areas.
- Backup power to cover 'living areas.'
- Evacuation routes and communication.

What you can do for your family

Build an emergency kit

- The basic kit recommended by the Federal Emergency Management Agency (FEMA) includes: battery powered radio with extra batteries; non-perishable food and drinking water; a first aid kit; soap, water, bleach and other sanitation supplies. These items are useful for dealing with all types of disasters, not just those related to terrorism.

- You'll also want to think about including in your kit a small amount of cash, a flashlight with fresh batteries, and any items that are essential to your health, such as prescription drugs.

Know who to contact

- Your family should establish an out-of-town contact to act as command central in the event of a disaster or "inconvenience." Make sure this person knows he or she is the emergency contact person and has essential phone numbers and e-mail addresses on hand.

- Family members should carry the family contact's phone number and e-mail with them at all times and plan on calling or e-mailing that person if they have problems getting in touch with each other directly.

Get an amateur radio license and get involved

- One day license session
  - www.arrl.org
  - www.w5yi.org
- Emergency communications training
  - www.arrl.org/cce

What you can do for your company

Start a business continuity planning program

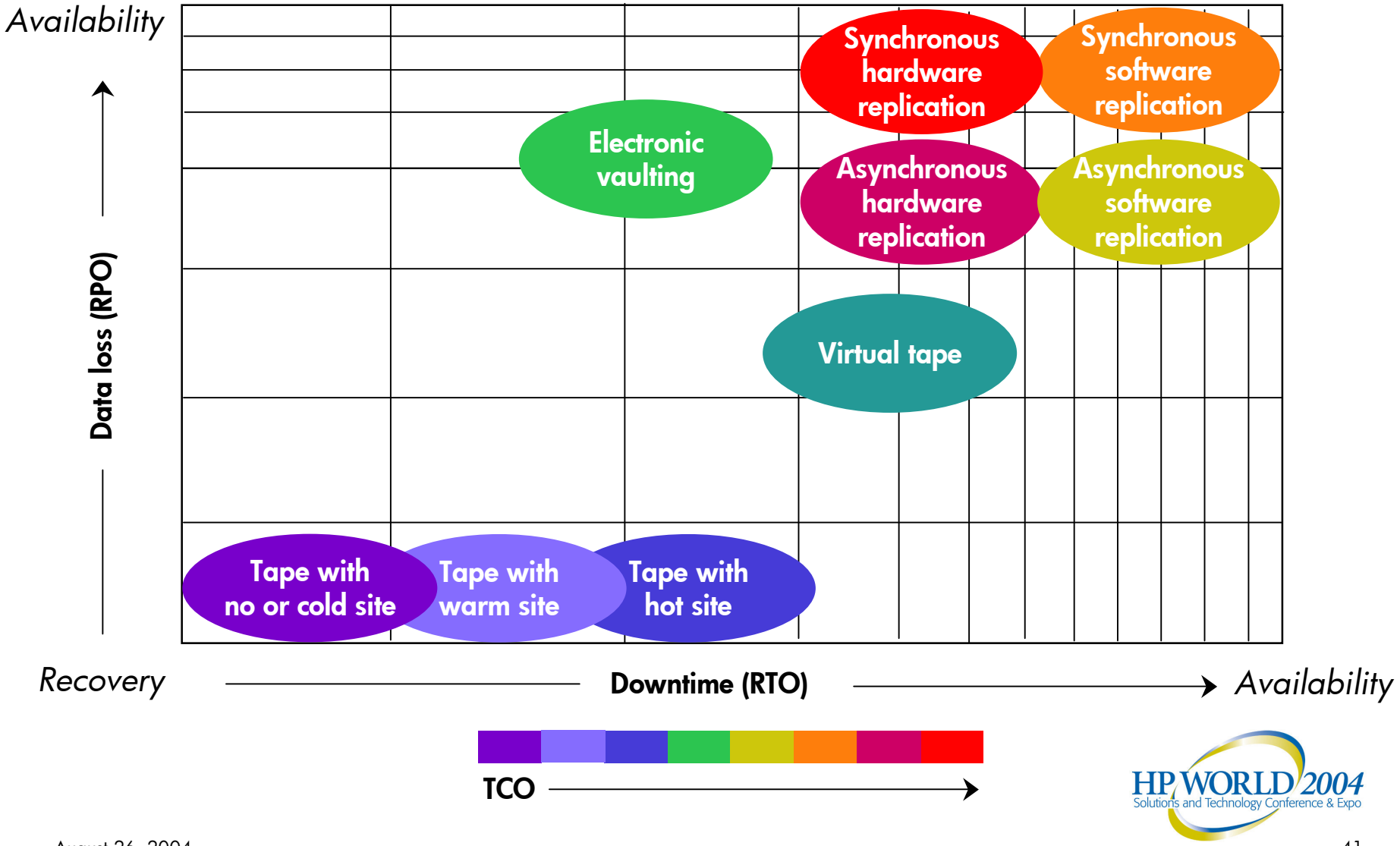
Does your company:

- have SOPs for *all* business processes?
- know what business processes are critical to its operation?
- know how long critical processes can stop before crisis sets in?
- know how much work in progress can be lost?

Downtime and data loss

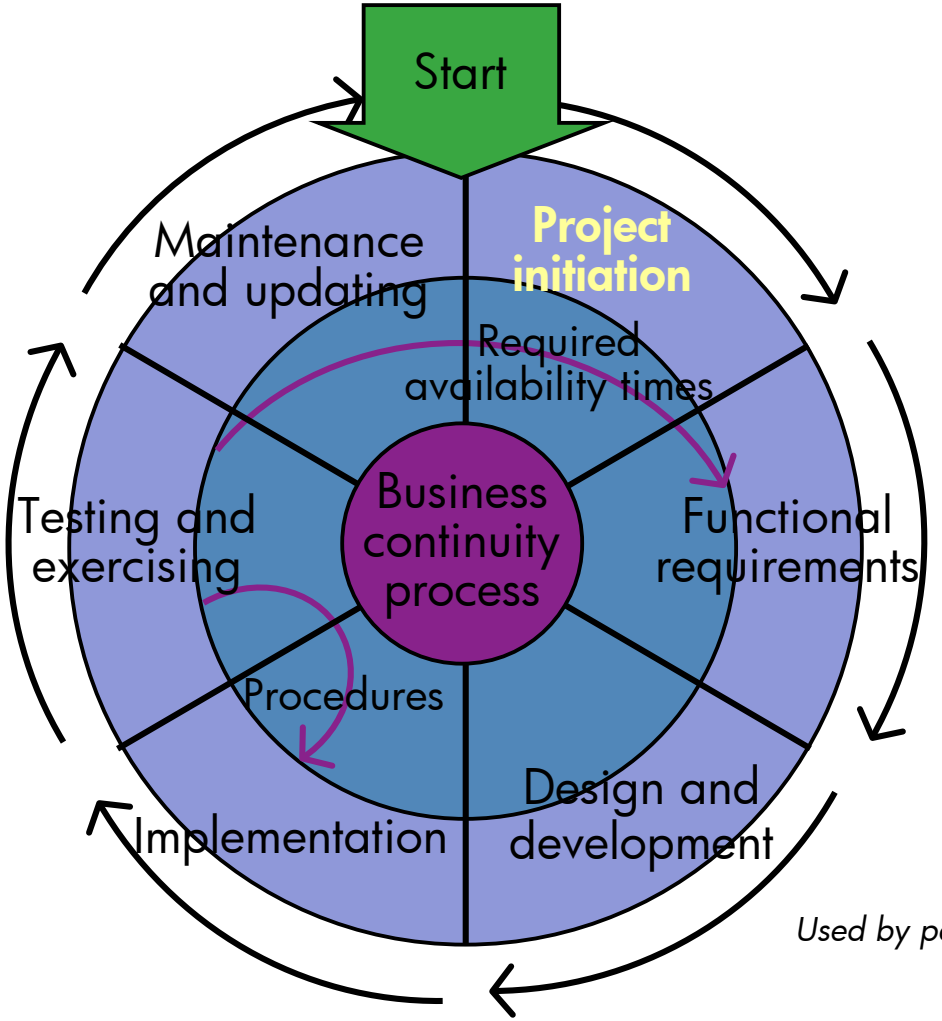
- RTO (recovery time objective)
  - How soon after an event does the business process need to be available?
  - Not all business processes need to be available at the same time.
- RPO (recovery point objective)
  - How much work in progress can be lost?
  - Not all work needs to be recovered to the same time.

Downtime and data loss



BCP is a long term process

- Session 3120 goes into more detail



Used by permission of DRI International

Disaster Tolerance should not be an afterthought

Disaster Tolerance solutions for NonStop servers

- HP Metrocluster for NonStop servers
  - Metrocluster allows NonStop servers to be geographically separated for disaster tolerance. ServerNet connections up to 15 km and RDF/ZLT connections up to 100 km are supported configurations.

- HP Continentalclusters for NonStop servers
  - Continentalclusters allows systems to be geographically separated over unlimited distances through the use of NonStop RDF over Expand networking for the ultimate in disaster tolerance.

Disaster Tolerance solutions for NonStop servers

Solution	Benefit	Data replication	Comms	Storage	Distance	Time
Basic disaster recovery	Low cost entry level	Tape backup or electronic vaulting	LAN, WAN	Any storage	Unlimited	1-7 days
Metrocluster with ServerNet	Local failover	NonStop RDF Host-based disk replication	ServerNet, DWDM, Fibre Channel	Internal disk StorageWorks XP ESS Nomadic Disk	15 km	1-60 minutes
Metrocluster with remote disk	Regional failover	NonStop RDF Host-based disk replication	DWDM, Fibre Channel, FC over WAN	Internal disk Remote StorageWorks XP ESS Nomadic Disk	ND – 30 km XP – 100 km	1-60 minutes
Continental-clusters	Unlimited distance failover	NonStop RDF	WAN	Internal disk StorageWorks XP ESS	Unlimited	1-60 minutes

Hire experts if you need them

- If you don't have the expertise to develop your own plan, hire professionals
  - HP HP HP HP

And finally …

- 43% percent of the businesses in the New York World Trade Center were out of business within a year of the 1993 bombing.
- 70% of the businesses that were in the towers, 90% of the businesses that were in the complex, as well as 162,000 jobs that existed on the morning of 9/11/2003, vanished by mid 2003.

For more information…

- http://www.hp.com/go/continuity
- http://www.hp.com/go/nonstopcontinuity

- **Product manager for security and continuity products for NonStop servers**
  - ron.lapedis@hp.com

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

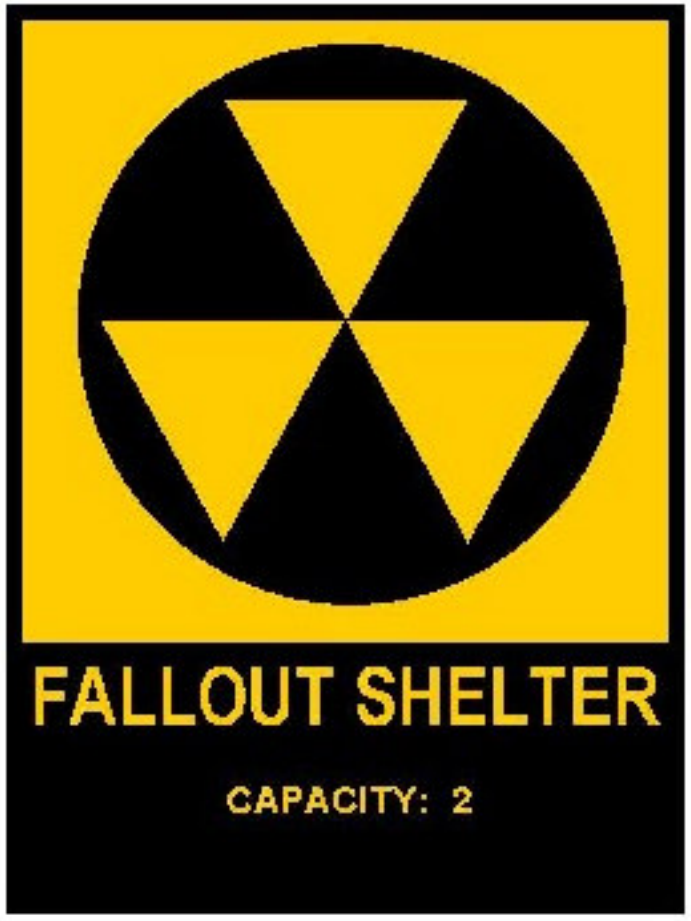
encompass

AN HP USER GROUP

RECOMMENDED TRAINING VENUE FOR THE

HP Certified Professional

Horror stories



Horror stories

- The backup site is in Atlantic city; declaration is during the Miss America pageant. (Hurricane Andrew)
- The computer room is in the basement, and there's
  a fire in the building. (Bell Canada)
- Will the generators be safe? Do you have a way to refuel them? (Tropical Storm Allison)

Food for thought

Tapes

- Where is your tape backup hardware?
- Where are tapes stored until they go off-site?
- How quickly do your tapes go off-site?
- Are multiple tape copies sent via different routes?
- Do you do tape retrieval and restore tests?
- For recovery, do you ship tapes in “waves”?

Food for thought

- The security code for pulling backup tapes from off-site storage is in your desk drawer.
- The phone number of your hot-site vendor is under a button in your auto dialer.
- What will you need that's stored in your Rolodex?
  - (Some people never learn.)

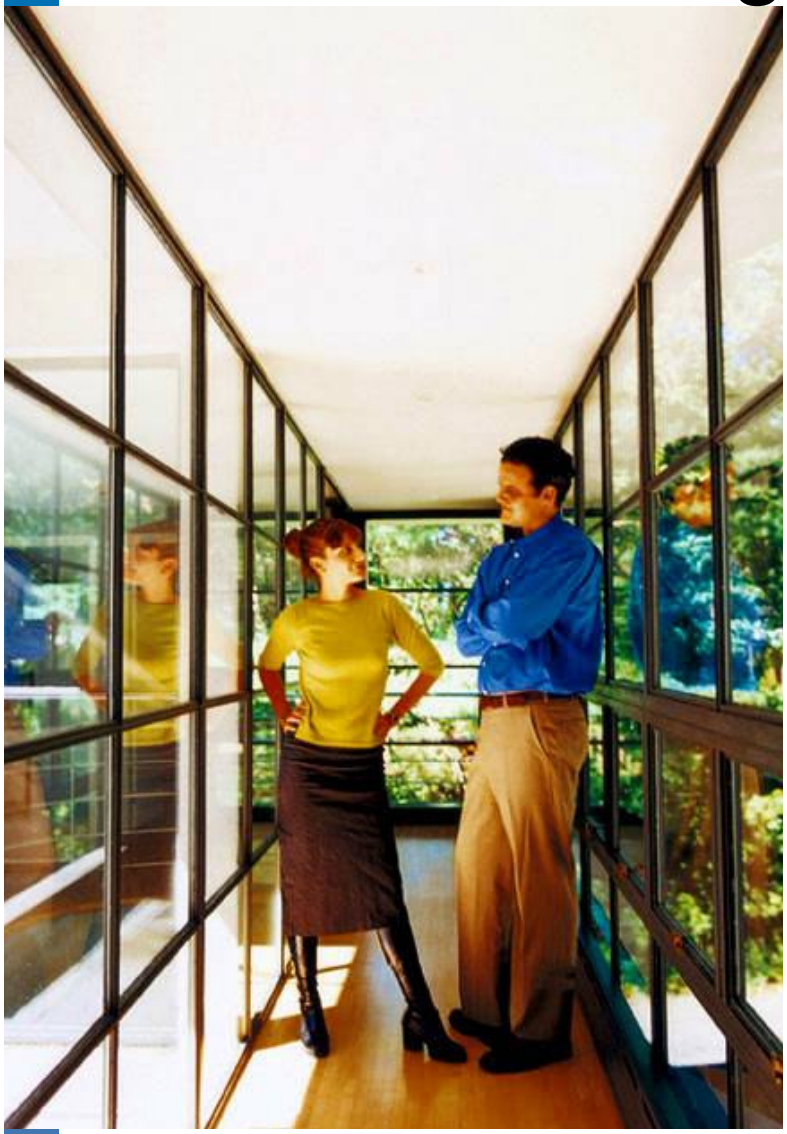
Food for thought

- Replicated enterprise storage
  - Vendors guarantee disk integrity.
    - Backup disk = primary disk at a bit level
  - Database integrity is *not* guaranteed.
  - Your OS needs to recover the crashed disk
  - Your database software needs to recover the database to a consistent state before you can begin processing on the backup system.

Food for thought

You updated your application and changed the database format.
The replication software will not work unless you change the database format on your backup system, but did you remember to copy over the new object files?

Food for thought



- Check your third-party site contract.
  - How many other companies in the same threat area use the same vendor?
  - How soon do you have to vacate? Where will you go?
  - Have you included workstations and allocated space for them?

And finally …

- 43% percent of the businesses in the New York World Trade Center were out of business within a year of the 1993 bombing.
- 70% of the businesses that were in the towers, 90% of the businesses that were in the complex, as well as 162,000 jobs that existed on the morning of 9/11/2003, vanished by mid 2003.

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP

RECOMMENDED TRAINING VENUE FOR THE

HP Certified Professional