Managing a Disaster: Getting Started with IT Crisis Management and Emergency Response Teams

Ellis Holman
IBM

Karla Houser

Session 10388

Abstract

When a disaster occurs, and there will be one someday, it is too late to start planning how you will manage the situation. Confusion in a stressful situation can very easily arise, and can be fatal. All companies need to prepare for crisis management and emergency responses during disasters such as IT and utility failures, terrorist attacks, fraud, sabotage, theft, flooding and fire. The aim of your overall disaster recovery plan is to enable your organization to protect its staff and assets during an incident, resume and maintain its key activities during the disruption and return swiftly to normal operations. However, the plans to manage the event, the process to formally declare an IT disaster, practicing how to work as a corporate team during the event and manage your ongoing event communications, etc. are often "forgotten" in the development of your detailed technical recovery plans. As real experiences have shown, planning for communications and risk mitigation during the event just does not work!

In this session, our speakers will focus on the activities required to develop, implement and test your IT focused Crisis Management plan(s) and the associated management team(s). No organization is immune to a crisis. Thus, a contingency plan must always be ready for overcome the crisis.

Join us to learn more about managing a crisis (with some real world examples) and some techniques you can apply if you find yourself in a crisis that impacts one of your data centers or if IT is impacted by the crisis. Who knows, you may even leave with an initial sample crisis management exercise to use!

Presentation Purpose

- To help you get started with implementing your IT focused Crisis Management plans:
  - Provide an overview of Crisis Management and Emergency Response Planning
  - Provide an overview of the steps needed to develop, implement and test your IT Crisis Management and Emergency Response plans
  - Provide brief descriptions of some real-world IT disasters

Disclaimer:

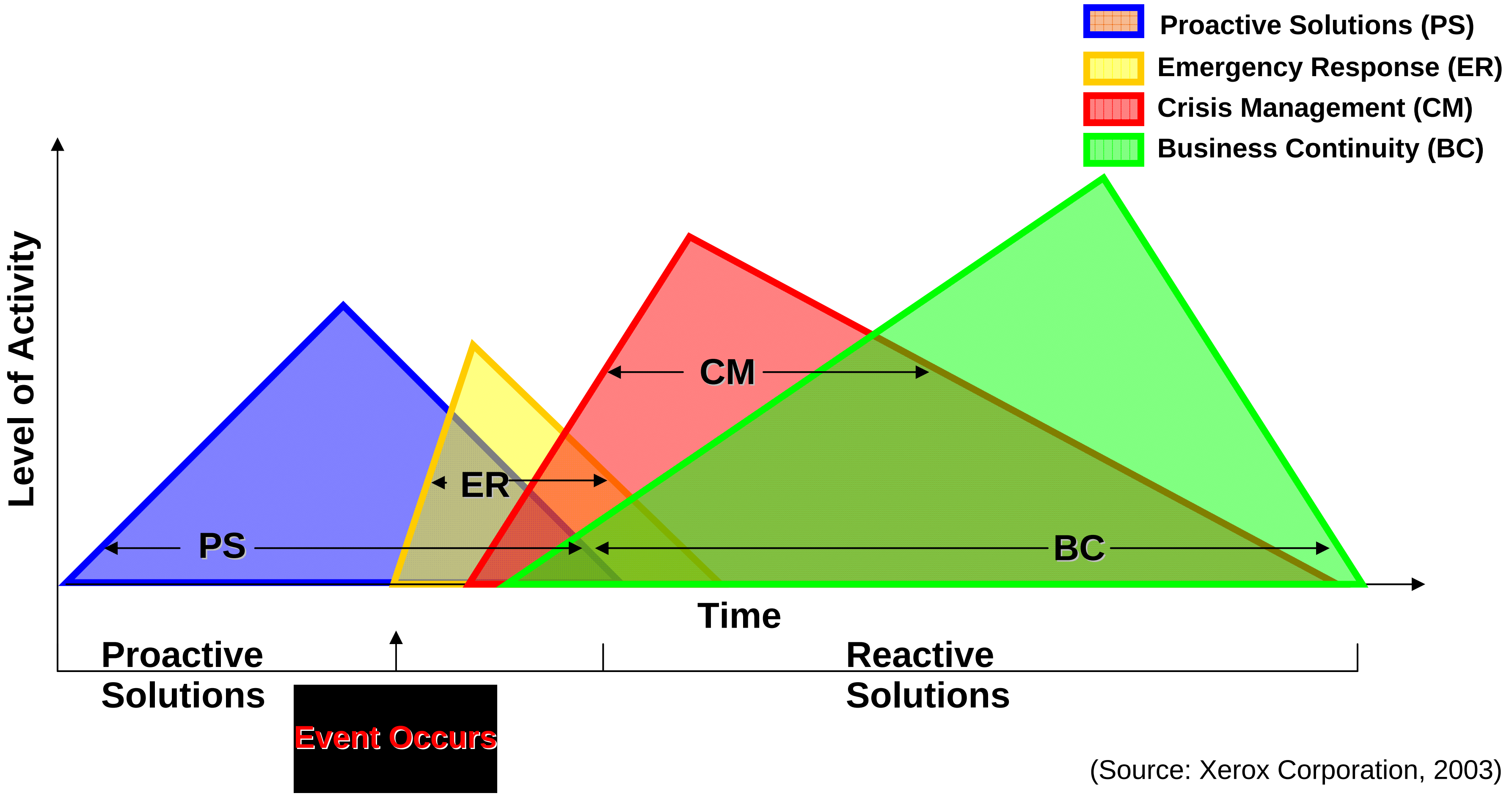
- *Speakers do not endorse any products/vendors.*
- *Speakers do not recommend the purchase of any products by the participants.*
- *Each participant should make up her or his own mind when evaluating the material.*
- *The views presented in this presentation are solely those of the speakers and not those of any company or organization.*

Agenda

- What is a Crisis?
- What is Crisis Management?
- Emergency Response Team
  - Organization & Structure
  - Roles and Responsibilities
  - Plans
- ERT Plan Exercises
- Real World IT Disasters

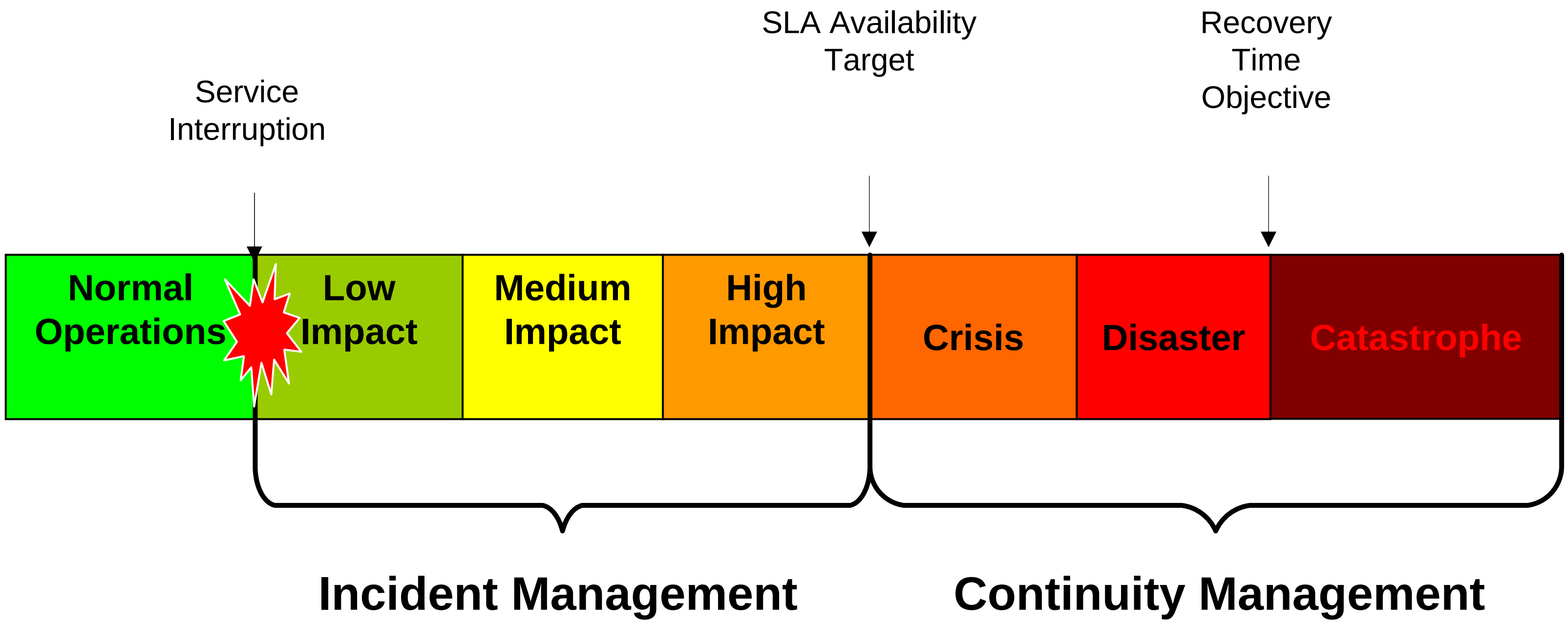
What is A Crisis?

Business Crisis Management - High Level Methodology



(Source: Xerox Corporation, 2003)

And an IT Perspective …



Service Interruption

SLA Availability Target

Recovery Time Objective

Normal Operations

Low Impact

Medium Impact

High Impact

Crisis

Disaster

Catastrophe

Incident Management

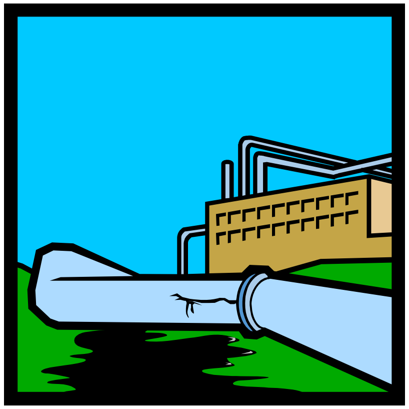
Continuity Management

A Crisis Is …

- An unexpected event that threatens the well being of a company
- A significant disruption to the company and its normal operations which impacts its customers, employees and/or investors
- Crises can be categorized
  - Fairly predictable and quantifiable crises, or
  - Totally unexpected crises
- Crises do not discriminate based on a company's size or notoriety
  - They can strike when you least expects them

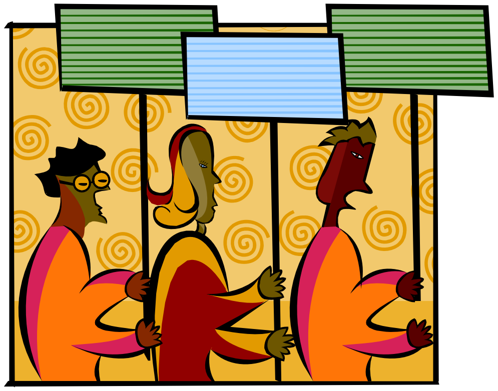
And IT Can Be Impacted By …

- **Natural disaster**
  - Physical destruction due to natural disaster
- **Industrial accident**
  - Construction collapse
  - Fire
  - Toxic release
- **Product or service failure**
  - Product recall – faulty or dangerous goods
  - Communications failure
  - Data Center failure
  - Machine failure that causes a massive reduction in capacity



And IT Can Be Impacted By …

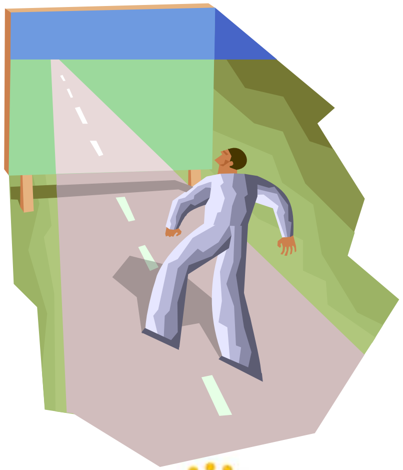
- **Public relations**
  - Unwelcome media attention, including social media
  - Adverse publicity in the media
  - Removal/loss of CEO or other key management
- **Business and management**
  - Hostile takeover
  - Sudden strike by your workforce or that of a key supplier
  - Major customer withdraws its support
  - Competitor launches new product
  - Sudden shortfall in demand
- **Legal**
  - Product liability
  - Employee or other fraud
  - Allegations of misconduct



Crisis Response Is Critical

- “The public forgives accidents, but it doesn't forgive a corporation if its response to the public is inadequate.” (James W. Burchill)

- Once a crisis occurs
  - Your company is a target for the media
    - Acting on behalf of the public to find out the answers to the important questions about their own safety
  - Your company must overcome the public's perception
    - Perception is reality
    - PR News, cites a survey that says 65% of the public views "no comment" as an admission of guilt



Crisis Response

- Time is at a premium during a crisis
- Essential to plan ahead
  - The wrong split-second decision can cost a company millions in negative publicity
  - Develop a crisis communication plan that outlines the steps to be taken during the first few hours of a crisis
    - Define the who, what, when, where and how your company should deal with the crises
    - Produce materials necessary ahead of time
      - Initial official statements
      - Press releases
      - Fact sheets
      - “Missing information” (fill in the blank) is okay
        - Later it can simply be inserted and the materials are ready to go
  - A good crisis plan is "everything you need in one place so you don't have to search”
    - You may not have time to search ☺

What is Crisis Management?

And why should I care?

Defining Crisis Management

- The art of making decisions to head off or mitigate the effects of a crisis, often while the event itself is unfolding
  - Often means making decisions about your business's future while you are under stress and while you lack key pieces of information
  - Can plan for and script
    - Cannot guarantee automatic control of a situation
    - Cannot cover all conceivable situations
    - Common sense and a logical interpretation of the situation must prevail
    - Decisions may change as more facts and data become available

Crisis Management Continuum

- **Planning**
  - Getting your business in the best position to react to, and recover from, an emergency
- **Incident Response**
  - Processes that you have put into place to ensure that your business reacts properly and orderly to an incident as it occurs. Examples:
    - Evacuation after a called-in bomb threat
    - Denial of entry to suspicious persons
    - Denial of service attack to your business’s web site
- **Crisis Management**
  - Management and coordination of your business’s responses to an incident that threatens to harm, or has harmed, your people, structures, ability to operate, valuables and/or reputation
    - Take into consideration planning and automatic incident response, but must also dynamically deal with situations as they unfold, often in unpredictable ways
- **Business Continuity**
  - The steps necessary to restore your institution to normal functioning

Planning Incident Response Crisis Management Business Continuity

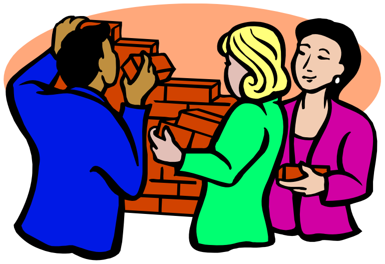
Crisis Management vs. Risk Management

- **Crisis Management Is Reactive**
  - Deals with threats after they have occurred
  - How you manage and cope with a serious situation from the moment it first occurs to the point that recovery procedures start
  - Get it under control and fix it quickly as possible
- **Risk Management Is Strategic**
  - Identification of potential threats
  - Assessment of their likelihood and their impact (if they were to occur)
  - Taking the necessary steps to eliminate or minimize them
- **But …**
  - The best laid risk management plans aren't going to prevent every crisis
    - **Stuff happens**
    - **So prepare**

However, I Only Care About IT

- Your IT is your business
- IT can be impacted by a crisis
  - Natural disasters
  - Hazardous waste spills
  - Equipment (data center) failures
  - Workplace Violence
  - Pandemics
  - Computer viruses and malware
  - …
- IT requires Crisis Management and the associated Emergency Response Team and Plans

Emergency Response Team and Plan



Emergency Response Plan

- **Roadmap** for action should an emergency impact your business
  - Prepared to minimize hazards to employees' health and safety, property, and the environment during emergencies such as fires, explosions, or natural disasters
  - Describes prudent, but proportional, actions your company personnel will take to ensure the safety your employees in the event an emergency should arise
  - Defines communications and "command and control"
  - Cannot guarantee automatic control of a situation, nor can it cover all conceivable situations
  - Common sense and a logical interpretation of the situation must prevail
  - Recognize that no written document can foresee all contingencies
    - Must expect that "on-site" decisions, based on experience, good common sense and a commitment to "do the right thing", must always prevail in times of emergency
- Do not presume that electronic copies of your plan are immediately available during an emergency situation

Emergency Response Team (ERT)

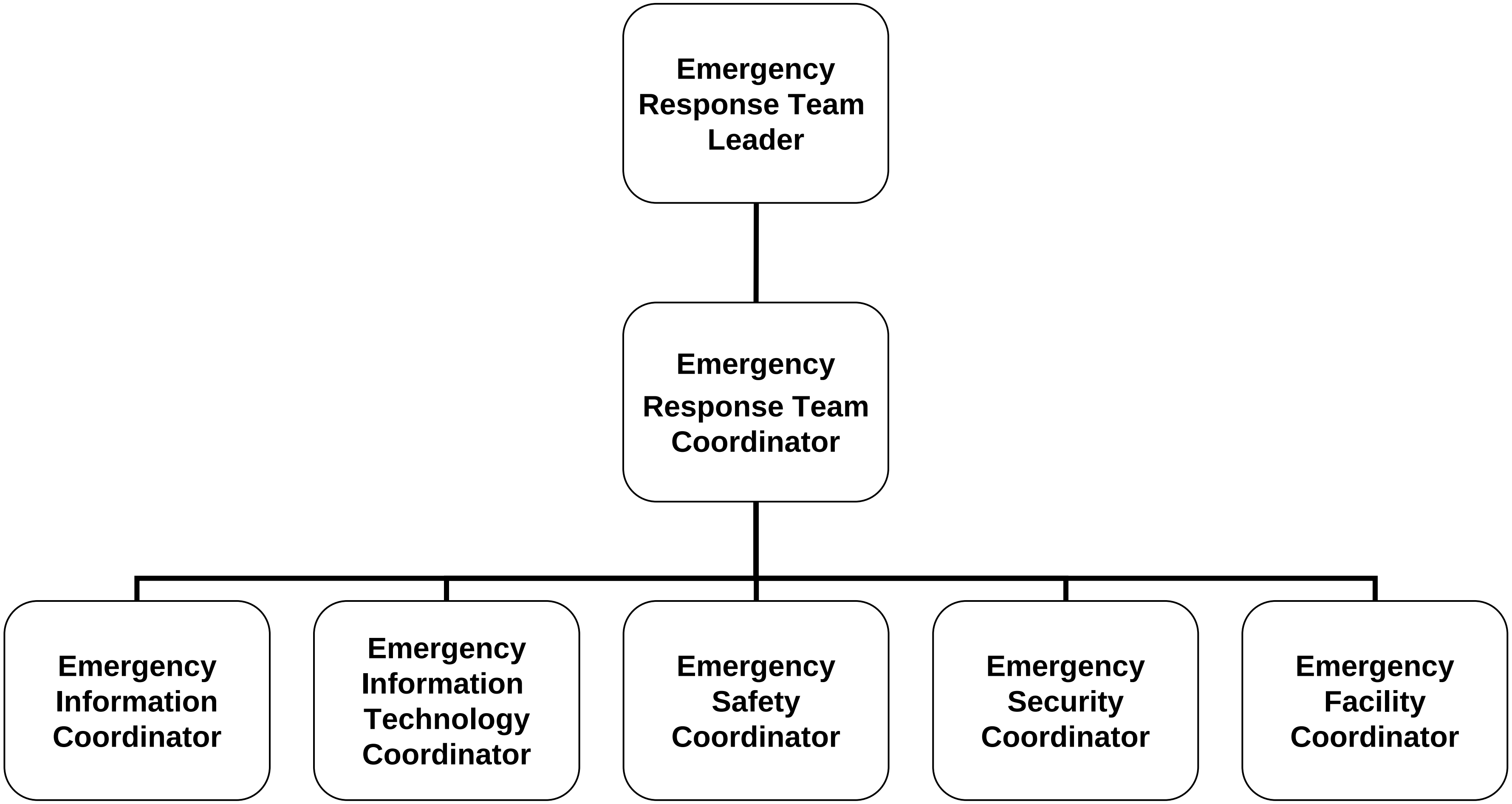
- The management team responsible for the management of emergency incidents
  - Executes the plan
  - Ensure adequate response to emergency situations

- Team Leader should be a Senior Level Manager
- Team Coordinator should be familiar with the site organization, administration and layouts

Emergency Response Team (ERT) (cont.)

- **Team should include:**
  - Senior management (decision making, business knowledge/focus)
  - Facilities management (locations and safety)
  - Human resources (personnel issues and travel)
  - Communications (media contact)
  - Finance/accounting (funds disbursement and financial decisions)
  - IT
  - Any other area appropriate for your business
- **Alternates must be named**
- **Membership can vary by crisis type**
  - Example - Workplace violence crisis may not require data center recovery team involvement

One Sample ERT Organization Structure


Emergency Response Team Leader
Emergency Response Team Coordinator
Emergency Information Coordinator
Emergency Information Technology Coordinator
Emergency Safety Coordinator
Emergency Security Coordinator
Emergency Facility Coordinator

ERT Team Member Characteristics

- Individuals should be able to make timely decisions
  - In some cases, instantaneously
  - Possibly based on limited information
  - Often without the support of others
  - Should have a history of “good” decision making
- Individuals should be flexible
  - As time goes on, facts and data may revise initial decisions
- Team members should work well with each other
  - An emergency is not the time for personality conflicts to arise
- Good communication skills
- Understand your business
- Ability to function well in stressful situations

Convening the ERT

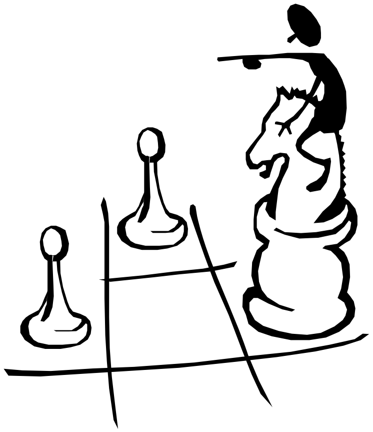
- Designate area(s) that serve as the base of operations during an emergency and are equipped with the necessary communication equipment and other devices needed to coordinate emergency response
  - Includes a copy of the ERP, facility site plan, evacuation routes and shelter-in-place areas
  - Should have adequate computer equipment and infrastructure as well as external and internal communication capability
  - Consider including a satellite phone for use when landline and cell phone services are interrupted
- However …
  - What if the emergency prevents you from assembling in the building – where do you meet?
  - Can you meet VIRTUALLY?
  - What if it happens in the middle of the night while everyone is at home…

ERT Plan Structure

- Definitions
- Member list (roles & responsibilities as well as names)
  - Notification methodologies (including phone numbers)
- Maps
- Incident report form
- Other forms
  - Hazardous materials, etc.
- Updates to plan format and delivery format

ERT Plan Structure (cont.)

- Process Overviews
  - List types of incidents addressed
    - Examples
      - Weather related incidents
      - Security & violence incidents
      - Medical incidents
      - Equipment failures
      - …
  - Process steps
    - Discovery
    - Notification
    - Response
    - Assessment
    - Planning
    - Action
    - Resolution
    - Evaluation
    - Corrective actions
  - Recognize that some of these incidents provide more of an opportunity to consult with the team before responding and others demand immediate action



Sample ERT Process Overview – Earthquake

- **Discovery**
  - Earthquake occurs
- **Notification**
  - Sound alarm
- **Response and Actions**
  - General information
    - If indoors, take shelter in pre-approved areas or under a heavy piece of furniture against an inside wall and stay inside
    - If outdoors, stay out of buildings and in an open area until shaking stops
    - If in a moving vehicle, stop quickly in open areas away from bridges and power lines
  - ERT leader documents time and location, gathers initial description of event
  - Evacuate all buildings to prevent injury/damage after-shocks (keep personnel out of buildings and take head count and report to ERT leader)

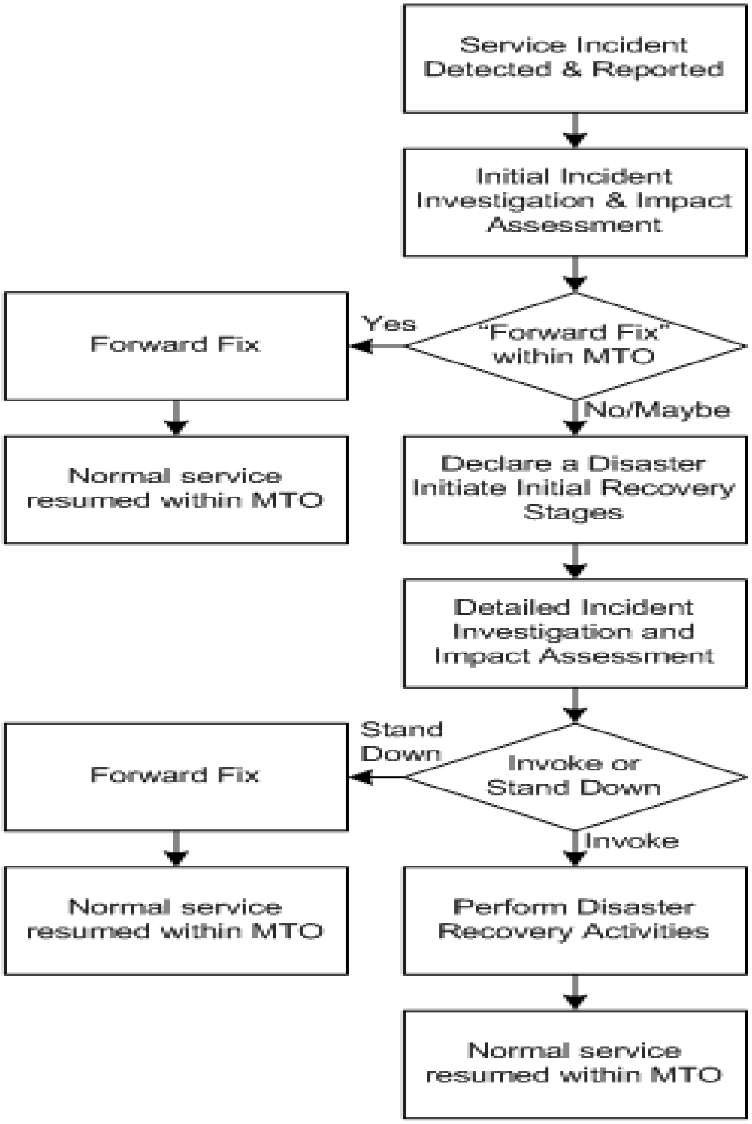
Sample ERT Process Overview – Earthquake (cont.)

- **Notification**
  - ERT leader notifies other ERT members
- **Assessment**
  - ERT members collect information on damage
  - ERT evaluates damage – is site safe, etc.
- **If damage – Action**
  - Account for personnel
    - Search and rescue, if required
  - Shut off all power and isolate all hazardous liquids
  - Begin safely extinguishing any small fires
  - Advise local authorities of conditions
  - Get outside assistance as needed to secure the property from fire, looting, etc.
  - Be prepared for aftershocks, which can cause additional damage
  - Provide for food and water if needed

Sample ERT Process Overview – Earthquake (cont.)

- **If no damage – Action**
  - Be prepared for aftershocks, which can cause additional damage
- **Assessment**
  - Complete reporting process
  - Complete damage and hazardous situation assessment forms
- **Resolution, Evaluation, Corrective Actions**
  - Debrief personnel
  - Review for lessons learned
  - Implement process improvements

Sample Disaster Declaration Flow



Service Incident Detected & Reported

Initial Incident Investigation & Impact Assessment

"Forward Fix" within MTO

Yes

Forward Fix

Normal service resumed within MTO

No/Maybe

Declare a Disaster Initiate Initial Recovery Stages

Detailed Incident Investigation and Impact Assessment

Invoke or Stand Down

Stand Down

Forward Fix

Normal service resumed within MTO

Invoke

Perform Disaster Recovery Activities

Normal service resumed within MTO

An incident is reported using the standard processes.

How serious is the incident and what is the impact to the business.

Can the critical services be forward fixed with the maximum tolerable outage (yes or no/ maybe)

Declaring a disaster at this stage will invoke the initial stages of recovery, You may invoke or stand down at a later stage

Understand the full impact of the incident. Assess if forward fixing within MTO is achievable or if recovery at an alternate site needs to be performed

Invoke full disaster recovery or stand down and forward fix

Perform full disaster recovery activities as detailed in the Disaster Recovery Plan

http://www.continuitycentral.com/feature0524.htm

IT Crisis Management and Disaster Recovery is Just A Really Big Incident ….. Right?

- Special actions may need to be taken in a crisis or disaster
  - Major changes in priorities
    - Production or application development?
    - What about scheduled changes?
  - Reallocation of resources
  - Offsite recovery
  - Health and safety concerns
  - Communication (internal and external)
  - Insurance claims
  - Investigations
  - Legal issues
  - Consultants/suppliers
  - Software keys
  - Other

Additional Items to Consider for an IT Disaster Recovery

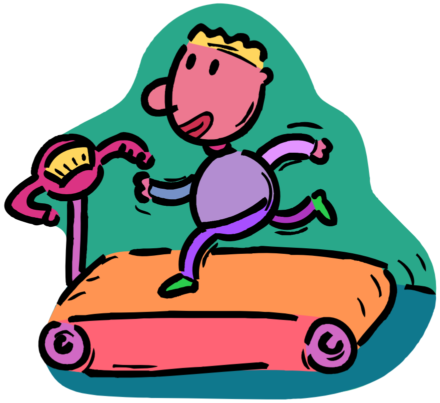
- What is the application recovery order?
- How are equipment lists maintained?
  - What infrastructure is needed?
  - When?
- What needs to be ordered at time of disaster?
  - Software and hardware
- What software may need to be re-installed?
- Impact of changes to lists? Are they really current?
- What about planned changes? Can they be delayed? Timeframe?
- Where is your data now backed up/mirrored to?
- Return to “normalcy”
- Return to “home” (or “new home”)

A Sample IT Disaster Declaration Aid

Decision Making Factor	Unlikely	Possible	Likely
Estimated downtime	< 4 hours	4 – 40 hours	> 40 hours
Impact to business considering workarounds (current or potential)	Isolated impact	Many impacted	Enterprise impact External customers
Public Relations	Internal impacts only	Extended enterprise impacts	Negative external exposure
Legal regulations	No threat to safety or financial reporting/ payroll	Possible impact to safety or financial reporting/payroll	Impact to safety or financial reporting/payroll
Contractual obligations	Within SLA agreements for availability, response time, capacity, etc.	Threaten ability to meet SLA or customer commitments	Will incur penalties for violating SLA, severe damage to customer relationship
Extent of damage (physical or data)	Little or no damage Easily/quickly repaired	Moderate damage; Extended downtime to repair	Substantial damage; Difficult/impossible/lengthy to repair
Workload	Under-utilized (eg. weekend, holiday, normal downtime)	Normal utilization	High utilization (eg. quarterly account closing)
Potential damage to equipment	Little or no threat	Possible damage without intervention	No way to prevent potential damage (eg. flood/levee)
Access to facility	Full access	Restricted access	Denial of access
Cost incurred by initiating recovery	$	$$	$$$
Impact of restoring service to normal ("return to home")	Major outage, cost, or risk	Significant outage, cost, or risk	Minor outage, cost, or risk

You must create your own table, based on your business requirements, recovery capabilities and business processes

ERT Responsibilities – Exercising Your Plan



Why Exercise?

- Identify Roles and Responsibilities
- Enhance skills, confidence and teamwork
- Assess capabilities
- Evaluate performance
- Determine gaps and overlaps
- Validate the written plan
- Train the team
- Eliminate the “It Can’t Happen Here” mentality

Sample Exercise Format

- Review your plan briefly
  - Review your process steps
    - Can be specific for the exercise type
- Conduct the table-top exercise
  - Objectives
  - Exercise
    - Develop scenario in advance
    - ERT perspective
    - Be prepared with possible discussion points
  - Document issues
  - Allow for discussion during and after
  - Critique
  - Action plans

Sample Exercise – Review Lessons Learned from Other Natural Disasters

- Japan - Lessons Learned from March 11, 2011
  - Re-evaluate longstanding assumptions
    - 2004 a 9.3 earthquake caused 98 ft tsunami in Indian Ocean
    - Fukushima plant designed for 8.7 earthquake / 19 ft tsunami
  - Consider cascading events in risk scenarios
    - Most prepared for earthquake/tsunami
    - Not prepared for combination
      - Nuclear crisis (power disruptions and shortages)
      - Transit disruption (days after only 50-75% trains running nationwide) impact on food and fuel supplies
      - Communications (undersea cable breaks cut 30% network capacity)

Forrester/IBM Webinar

Sample Exercise – Review Lessons Learned from Other Natural Disasters

- Japan - Lessons Learned from March 11, 2011
  - Plan for an extended duration
    - Aftershocks and nuclear crisis for weeks
    - Rolling blackouts for foreseeable future
  - Prepare for the loss of critical infrastructure
    - For days, companies struggled to gain access to:
      - Food and clean water
      - Fuel for their own diesel power generators
      - Telecommunication services
      - Mobile networks
      - Electricity

Sample Exercise – Review Lessons Learned from Other Natural Disasters

- Japan - Lessons Learned from March 11, 2011
  - Validate the readiness of critical partners and suppliers
    - Large companies rely on as many as 400 third party relationships for continued operations
      - Validate BC/DR readiness during selection and ongoing management
      - Potentially include in BC/DR testing
  - Third party relationships critical to deliver IT infrastructure, services, and fuel for backup generators
    - Organizations without a reliable supply chain for fuel were out of luck
    - Transportation disruptions impacted companies without documented quick ship arrangements with IT suppliers

Sample Exercise – Review Lessons Learned from Other Natural Disasters

- Japan - Lessons Learned from March 11, 2011
  - Employees are people first, employees second
    - Foremost, concerned with health and safety of families and themselves
      - Don’t assume employees will want to come back to work immediately
    - Focus on the long-term health and safety, but still allow for productivity:
      - Have an evacuation plan for employees to leave the region if they want to (especially if not from the region)
      - Shift the workload to another region

Sample Exercise – Review Lessons Learned from Other Natural Disasters

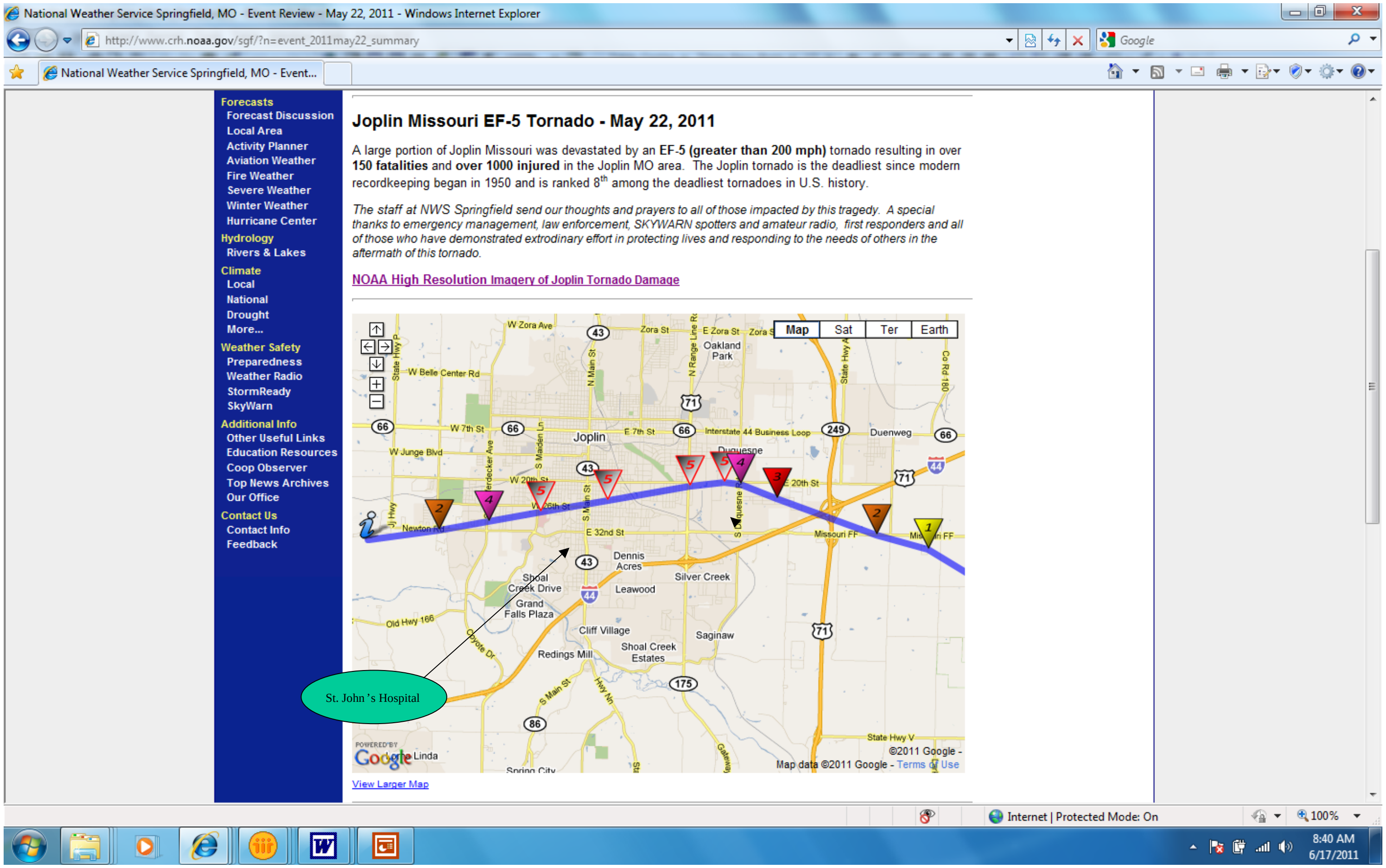
- Japan - Lessons Learned from March 11, 2011
  - Develop robust communication strategies using multiple modes
    - Use multiple modes of communication and ideally, automate it
      - Combination of landlines, mobile phone, SMS text, satellite phones, radio, email etc.
      - Subscribe to automated communication services
    - Leverage social media to your advantage
      - There are security and risk concerns
      - It is a valuable communication tool
      - Employees will use it either way, so it’s better to craft a strategy now

Sample Exercise – Review Lessons Learned from Other Natural Disasters

- Japan - Lessons Learned from March 11, 2011
  - Do you have a BC/DR plan in place?
    - Almost 80% of companies have a formal and documented DR plan in place
  - How often do you test your BC/DR plan?
    - **Less than a third of companies** follow the best practice of doing a full DR test at least twice a year
  - Do you keep your plans up to date?
    - **Almost half of companies** update their plans once per year or less
    - The best practice is to update plans continually as part of the change management process

Sample Exercise - Tornado

Review the nature of Severe Weather Emergencies



Joplin Missouri EF-5 Tornado - May 22, 2011

A large portion of Joplin Missouri was devastated by an **EF-5 (greater than 200 mph)** tornado resulting in over **150 fatalities** and **over 1000 injured** in the Joplin MO area. The Joplin tornado is the deadliest since modern recordkeeping began in 1950 and is ranked 8th among the deadliest tornadoes in U.S. history.

The staff at NWS Springfield send our thoughts and prayers to all of those impacted by this tragedy. A special thanks to emergency management, law enforcement, SKYWARN spotters and amateur radio, first responders and all of those who have demonstrated extrodinary effort in protecting lives and responding to the needs of others in the aftermath of this tornado.

NOAA High Resolution Imagery of Joplin Tornado Damage

Sample Exercise - Tornado

- The enhanced Fujita scale classifies tornadoes into the following categories:
  - EF0 - wind speeds 65 to 85 mph
  - EF1 - wind speeds 86 to 110 mph
  - EF2 - wind speeds 111 to 135 mph
  - EF3 - wind speeds 136 to 165 mph
  - EF4 - wind speeds 166 to 200 mph
  - EF5 - wind speeds greater than 200 mph

Sample Exercise – Tornado Warning and Watch Definitions

- Tornado Watch
  - Notification of a large area of atmospheric disturbance in which the conditions are favorable for an occurrence of a tornado or other severe windstorms from a specific geographical area. Such an area is usually from one hundred to several hundred square miles.
- Tornado Warning
  - Notification of a more confined area of probable tornado activity. Such an area is normally in the immediate vicinity of a city. It is also a notification that a tornado has been sighted or is in progress.

Why “Exercise” and not “Test”?

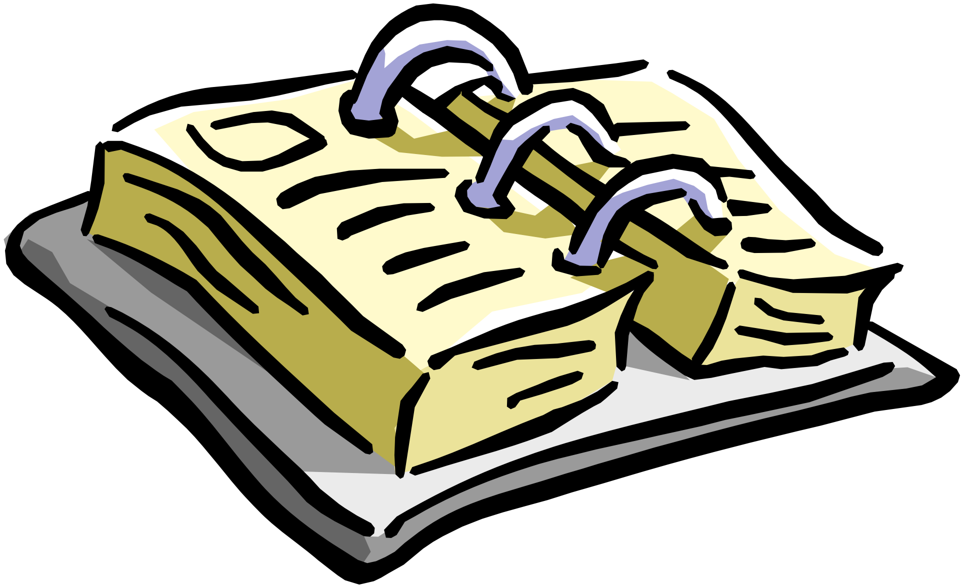
- Test
  - Conveys a pass or fail mentality
- Exercise
  - Does not imply pass or fail
  - Provides learning experience
- Emergency
  - Real test

ERT Team Role During An Exercise

- Perform your role as a member of the team
  - Focus on the “big” picture, not the “is xyz server down” items
- Focus on tactical response procedures
- Know when to take the response to the next level in the escalation process
- Read the narrative slides and then discuss within your team how your ERT would respond
  - You know what you know … nothing more or less
- Do not fight the scenario
  - Very important … sometimes the exercises may not seem plausible
- Document what you would do when
- Comment and discuss after the exercise
- Capture issues during the exercise and communicate them after the exercise

And now, the fun begins …

Monday, March 12



Scenario: 09:00 a.m.

A fire occurred and the building evacuation has completed.

Emergency responders are onsite and putting out the fire in the dining center and surrounding office areas.

The data center is still physically operational.

Pause … and discuss

- What would you do (as the ERT) at this point in time?
- Think about:
  - Where are you?
  - Where are the other members of the ERT?
  - How are you communicating?
  - What actions do you take at this point in time?
  - Do you do anything yet?
  - Weather outside … any special actions?
  - Do you have cell phone, car keys, laptop, coat, etc.?

Scenario: 10:00 a.m.

Emergency responders are onsite and have put out the fire in the dining center and surrounding office areas.

Select employees are being allowed back in to some of the areas of the facility.

Employees are still not being allowed back into the office areas of the facility.

The data center is still physically operational.

Pause … and discuss

- What would you do (as the ERT) at this point in time?

- Think about:
  - How do you handle the volume of people still outside?
  - How is the communication working within the ERT?
    - Have members of the team not on-site been notified?
  - What do you do if people want to leave the facility?
  - Do you have an IT sub team? If so, when are they notified?

Scenario: 13:00 p.m.

The damage assessment is continuing. Numerous cubicles will be uninhabitable for at least 48 hours.

Employees are still not being allowed back into the office area of the facility.

The data center is still physically operational.

Pause … and discuss

- What would you do (as the ERT) at this point in time?

- Think about:
  - How do you handle the volume of staff still outside?
  - How do you handle the staff that cannot use their normal work area for at least 48 hours?
  - How is the communication flow within IT working?
  - Do you take “preventative” IT actions … extra backups, etc.?
  - Can people even get home?
    - Do they have their personal cell phone, car keys, etc.?
  - How do you support the continued operation of your business?
    - Work from home … personal PC’s? Did people evacuate with their laptops?
    - Have you arranged for workspace, phones and desktops in other locations?
    - Do you have pre-defined other locations for support and staff work areas?
    - Ongoing communications to staff?

Scenario: Tuesday, March 13, 07:00 a.m.

The damage assessment is continuing.

Employees are still not being allowed back into the impacted office areas of the facility.

A critical business process has “paused” because a file required for its completion is only on a hard drive on a PC in the impacted area. The requested PC is still powered down and not accessible.

Pause … and discuss

- What would you do (as the ERT) at this point in time?
- Think about:
  - How do you support your business processes since laptops and desktops are inaccessible and possibly damaged?
  - Where are your “impacted employees” working from?
  - How is the communication flow working?

Scenario: Wednesday, March 14, 13:00 p.m.

The initial damage assessment is complete.

Employees are now being allowed back into the impacted office area of the facility. Many of the PCs (desktops and laptops) and phones in the impacted area have experienced water and/or smoke damage.

An analysis of the data center shows that the IT equipment is still running normally. However, there is still a "fire odor" in the data center. Visually the data center the equipment seems clean, but some black dust appears on hands when touching equipment.

A data center "damage assessment" team has been engaged.

Pause … and discuss

- What would you do (as the ERT) at this point in time?

- Think about:
  - How do you support your business processes since phones, laptops and desktops are damaged?
    - How are you handling “staff frustration” issues due to lack of IT assets? (IT and non-IT personnel)
  - Where are your “impacted employees” working from?
  - How do you deal with the potential data center issues?
  - How are the service centers functioning?
    - You are number #### in the queue … the estimated wait time is xxxx?
    - Service center staffing to assist with the increased call volumes?
    - Call prioritization changes? Front-end message changes ATOD?
    - Support team monitoring incident queues?

Scenario: Wednesday, March 14, 17:00 p.m.

The damage assessment team (including vendors) recommends that the data center be “cleansed”.

The process to cleanse the data center has been defined. The cleansing process impacts redundancy during the outage and dismantling/rebuilding IT equipment (server, router, cabling, ...).

When do we schedule the “planned” remediation activities for the data center?

Your quarterly infrastructure change weekend is two weekends away. This is the next planned outage.

A major IT business application has a critical upgrade scheduled for the weekend after that.

Pause … and discuss

- What would you do (as the ERT) at this point in time?

- Think about:
  - How do you deal with the upcoming data center “cleansing” process?
  - What about already scheduled changes during the existing change windows?
  - Do you consider adding additional change window(s)?
  - How is the communication flow working?

Review The Exercise

- Questions and comments for your ERT
  - Were there additional considerations?
  - How did your team perform?
  - What lessons did you learn?
  - What were the team’s strong points?
  - What needs improvement?
  - Who received action items?

And Now, Some Real World Experiences

San Francisco Power Outage - 2007

- A power outage hit downtown San Francisco on July 24, knocking out 365 Main Inc. — a 227,000 square-foot facility and datacenter development company.
  - At least three of 365 Main's eight co-location centers were knocked out. Among the Web sites that went down for a few hours were giants like Craigslist, GameSpot, Yelp, Technorati, Typepad and Netflix.
  - The backup generators did not kick in.
  - Power was restored after 45 minutes.
- 365 Main later estimated that between 20 and 40 percent of its customers were affected.
- The company ultimately attributed the disaster to backup generators that failed to kick in.
  - It seems that an incorrect setting in one tiny generator component prevented the component’s memory from resetting properly.

    http://www.itmanagement.com/features/top-8-012808/

Explosion Near Data Center

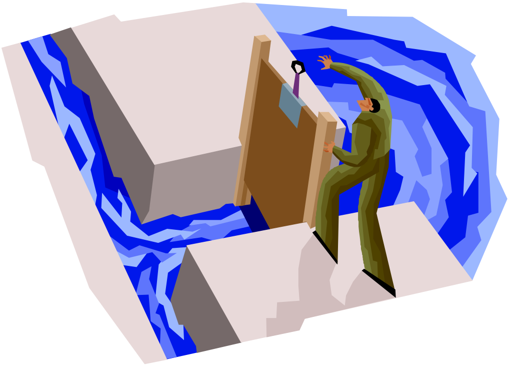
- A data center in the Midwest experienced a disaster situation in 2010.
  - A buried fuel oil pipeline existed 500 yards/450 meters from the data center. The company’s insurance company said it was ‘not a problem’. A backhoe digging a trench for the new power lines hit the pipe, punctured it and ignited the fuel oil inside.
  - Heat from the fire blackened the paint on some of the cars nearest the fire.
  - The decision was made to sound the fire alarm and move employees out of the immediate path of the fire.
  - The fire spread to employee vehicles. Explosions from burning vehicles sent shrapnel through the parking lot and sides of the building.

Explosion Near Data Center

- Some people, including those supporting critical IT functions, tried to leave the facility rather than staying inside. Other people attempted to recover belongings from vehicles.
- Once the “all clear” was sounded, the ERT began their damage assessment process. Power lines were down due to the fire and the parking lot was littered with debris and damaged vehicles.
- A data center disaster was declared and recovery processes started due to the power outages.

Are You Prepared?

National Flood Safety Awareness Week, March 12-16



"Floods can happen at any time, anywhere across the United States, which means we all need to be prepared now," said FEMA Administrator Craig Fugate.

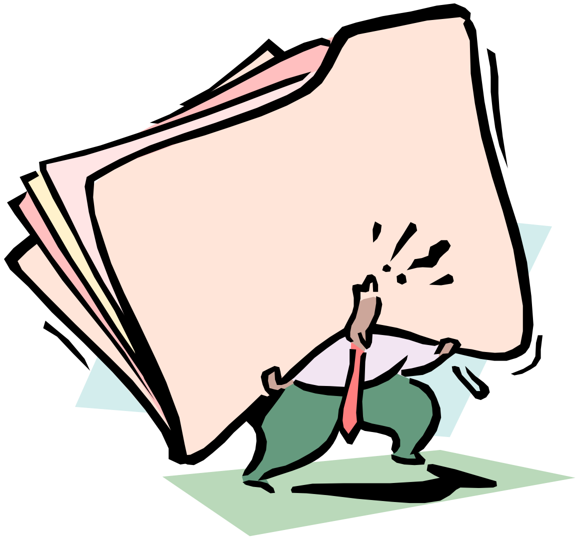
2012 Spring Flood Forecast will be issued Thursday March 15th at 9:00 AM.
For specific river forecast information, go to water.weather.gov

www.**oregonemergency.com**/.../2010/OEMA2010_BS5_FloodsFun.ppt

Questions and Answers

???

Additional Information



Some Useful Links

- Helpful sites and additional information
  - http://www.epa.gov/safewater/watersecurity/pubs/small_medium_ERP_guidance040704.pdf
  - http://www.nclabor.com/osha/consult/sampleprograms/hazwop.pdf
  - http://www.bt.cdc.gov/
  - http://www.fema.gov/plan/index.shtm
  - http://searchdisasterrecovery.techtarget.com/feature/Recovering-from-a-disaster-A-data-center-checklist
  - http://en.wikipedia.org/wiki/Crisis_management
  - http://www.continuitycentral.com/EmergencyProcedures%20FlowCharts.pdf
  - http://www.slideshare.net/Nostrad/crisis-management-3898059
  - http://www.fin.ucar.edu/sass/bc/BC-newsletterDeclaringAnEmergency.pdf
  - http://www.youtube.com/watch?v=aud-TEoJjf0&feature=related
  - http://www.docstoc.com/docs/73865501/Data-Center-Recovery-Flowchart
  - http://www.continuitycentral.com/EmergencyProcedures%20FlowCharts.pdf
  - http://www.complianceforbankers.com/ifs-industry-insight/bcp_1.pdf
  - http://inboundmarketingpr.com/Blog/bid/40716/BP-s-Social-Media-Disaster-4-Examples-of-What-Not-to-Do
  - http://www.jdcc.or.jp/english/DCD%20Presentation%20by%20Yamanaka%20%28Final%29%2020110630.pdf

- Search for “emergency response plan”
  - Will find plans from various organizations …

Terminology

- Disruption
  - Unplanned event that interrupts the normal flow of a business service for an appreciable length of time
- Disaster
  - Disruption of a critical business service or set of business services for an appreciable length of time
    - Unique to each installation
- Incident Management Plan
  - Documented procedures for recovering a business service from a short term disruption
- IT Disaster Recovery Plan
  - Documented strategy for recovering the IT infrastructure or IT business application after a disaster

Terminology

- Business Continuity Plan
  - “DR” plan that focuses on the business processes rather than the IT infrastructure
- Recovery Time Objective (RTO)
  - How long business process can be without IT application before significant damage to finances or reputation occurs or where required by legal or regulatory requirements
- Recovery Point Objective (RPO)
  - How much data the business process can recreate or afford to loose
- Maximum Tolerable Outage (MTO)
  - The **maximum** amount of time that the business can survive without the business process in any form (manual or automated)

Some Known Causes for Disasters

A/C Failure
Acid Leak
Asbestos
Bomb Threat
Bomb Blast
Brown Out
Burst Pipe
Cable Cut
Chemical Spill
CO Fire
Condensation
Construction
Coolant Leak
Cooling Tower Leak
Corrupted Data
Diesel Generator
Earthquake
Electrical Short
Epidemic

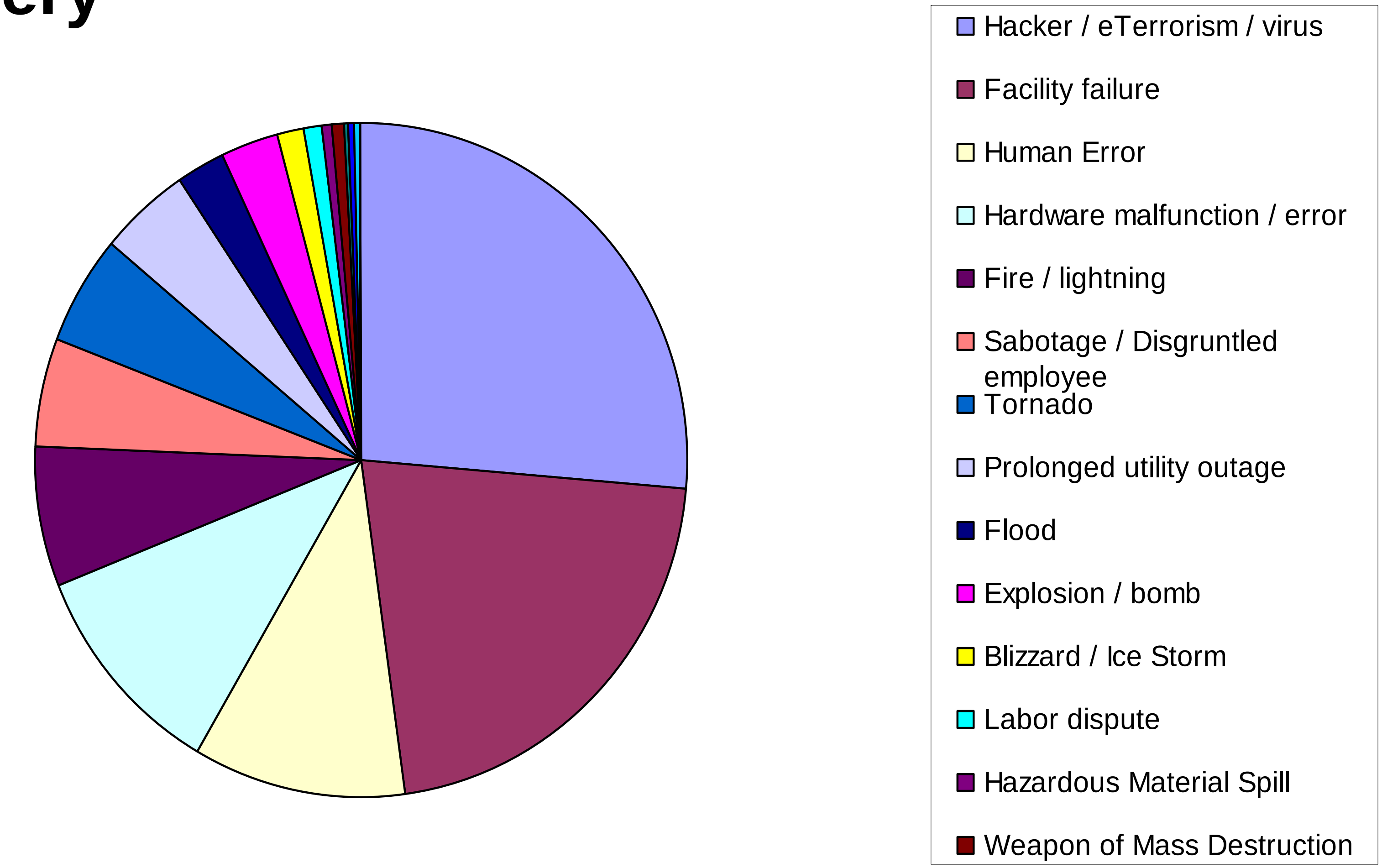
Evacuation
Explosion
Fire
Flood
Fraud
Frozen Pipes
Hacker
Hail Storm
Halon Discharge
Human Error
Humidity
Hurricane
HVAC Failure
H/W Error
Ice Storm
Insects
Lightning
Logic Bomb
Lost Data

Low Voltage
Microwave Fade
Network Failure
PCB Contamination
Plane Crash
Power Outage
Power Spike
Power Surge
Programmer Error
Raw Sewage
Relocation Delay
Rodents
Roof Cave In
Sabotage
Shotgun Blast
Shredded Data
Sick building
Smoke Damage
Snow Storm

Sprinkler Discharge
Static Electricity
Strike Action
S/W Error
S/W Ransom
Terrorism
Theft
Toilet Overflow
Tornado
Train Derailment
Transformer Fire
UPS Failure
Vandalism
Vehicle Crash
Virus
Water (Various)
Wind Storm
Volcano

Source: Contingency Planning Research, Inc.

Sample Disaster Profile – Relative Likelihood of Causing a Remote Recovery



10 Rules for Crisis Communications

1. Have an in-depth crisis communications plan that includes dealing with the media, the community and your employees.
2. Make sure the crisis team has been professionally trained in doing hard news interviews.
3. Name a spokesperson and a couple of back-ups now. Don't wait for the crisis to occur.
4. Deal with the crisis head-on. Don't hide from it.
5. Respond to reporters' questions immediately. They expect a return call or an on-site interview within 10 minutes of the request.
6. Never lie.
7. Never go off the record. In a crisis there is already much confusion. Do not add to it. Tell a reporter only what you want to see on the front page of the of your local newspaper (or the Wall Street Journal).
8. Have media kits already prepared and in the crisis room ready for distribution.
9. Practice implementing your crisis plan by going through a mock crisis periodically (annually). Don't forget the news media element during the practice.
10. Be prepared.

Source: Bill Patterson

Sample ERT Roles & Responsibilities

- Emergency Response Team Leader
  - Usually a senior executive
  - Responsible for
    - Coordinating all emergency functions
    - Maintain a current Emergency Response Plan
    - Evaluate risk and develop response procedures
    - Test facility Emergency Response Plan and conduct drills, as needed
    - Activate the Emergency Response Plan
    - Lead the emergency response
- Emergency Response Coordinator
  - Administrative and liaison aspects of emergency response
  - Usually in the office on a regular basis and have infrequent business travel
  - Responsible for
    - Ensure notification of the local government authorities of an emergency
    - Maintain communication systems during an emergency aligned with Business Continuity Planning
    - Receive and disseminate information about an emergency situation
    - Prevent unauthorized entry into hazardous or secured areas
    - Coordinate shutdown and start-up procedures with the appropriate personnel
    - Ensure that vital records are protected from the effects of a disaster
    - Assist with disaster assessment as required
    - Follow up with appropriate notifications to governmental regulatory agencies
    - Assess the incident and make recommendations to revise the ERP

Sample Exercise Issues Log

Issue #	Issue Description	Status	Assigned To	Target Date	Close Date	Notes