Disaster Recovery Incident Management

Ernest Schirmer, Senior Associate

WSP | Parsons Brinckerhoff
Incident Management: Terminology

Disaster Recovery Planning

Is Better Termed

Business Continuity Planning

or

Business Resiliency Planning

Why?
Incident Management: Terminology

Because “Disaster Recovery” implies events that are rare and dramatic: it may be very tough to convince management these events will ever happen. “Business Continuity” or “Business Resiliency” better describes the planning required to deal with everything from a broken copier to an earthquake.
Note: When some organizations use the term “disaster recovery planning” they are referring only to their data networks and computer systems since these are highly visible, obvious, mission-critical assets. But business continuity planning really covers everything from a broken copier to the total loss of facilities.
Incident Management: Defined

Incident Management: provides, organizes and controls physical and human assets and other resources to optimize an organization’s ability to efficiently and effectively control, manage and recover from interruptions.
Incident Management: Success Factors

Incident Command
Critical Success Factors

Command, Control & Communications

Converting

Data \text{ Into } Information \text{ Into } Action

Don’t confuse activity with accomplishment.
Incident Management: Success Factors

Operational Success Factors: The right mix of strategy and tactics.

**Strategy:** Put out the fire.  **Tactic:** Put the wet stuff on the red stuff.

**Strategy:** Get lines to the second floor.  **Tactic:** Safe to use stairs?

Real-time Analysis
Is the smoke the right color?
Volume of fire?
Exposures?
What size lines?
Incident Management: Planning

"I think we may need to update our disaster recovery plan. This one suggests we all run around in circles shouting 'what do we do?!' 'what do we do?!'

Our Disaster Recovery Plan Goes Something Like This..."
Incident Management: Bad Planning

*The Logic of Failure: Recognizing and Avoiding Error In Complex Situations*

Author: Dietrich Dorner

Publisher: Basic Books Rev. Ed. (1997)

240 pages

Incident Management

Justifying the Plan
Incident Management: Plan Justification

- Building the Economic Model
- Estimating the Probability
- Estimating the Consequences
- Estimating the Cost
- Redundancy
Incident Management: Plan Justification

• Remember, there are direct losses (revenue, profits) and indirect losses (customers and market share).

• How fast can your competitor’s product or service replace you?
Incident Management: Plan Justification

Which factors do you include in the cost of downtime

- SLA Penalties: 16%
- Goods and materials lost: 19%
- Regulatory compliance exposure: 26%
- Risk of litigation: 49%
- Remediation efforts: 53%
- Sales revenue/transaction value lost: 55%
- Upstream/downstream impact on others: 58%
- Restarting and returning to full operations: 60%
- Damage to organization's reputation: 62%
- Full carrying cost of impacted employees: 64%
- Customer dissatisfaction: 71%
- Number of admins and manpower hours: 76%
Incident Management

Business Impact Analysis
Incident Management

Risk = Threat X Vulnerability X Cost

Threat = probability of event happening

Vulnerability = probability of event to interfere with business

Cost = direct and indirect cost of event
Incident Management

Statistical calculation
Vendor data
SWAG

Note: Probabilities are based on incidents over a long period of time. Once in ten years doesn’t mean it can’t happen ten years in a row!
Incident Management

ESTIMATING THE PROBABILITY

• Redundancy \((N, N+1, N+2)\)

• Reliability \(\text{(MTBF)}\)

• \textbf{MTBF: Mean Time Between Failure}\(^*\)
  \(^*\)normally specified in hours
Incident Management

ESTIMATING THE PROBABILITY

• Availability (out-of-service vs. in-service hours)

• Survivability (what percentage of system can fail and still function)

• **MTTR:** Mean Time To Repair
Incident Management

Scenario: Justify the cost of diversity routing for telephone service.

- 600 sales calls per hour
- $25 average sale per call
- $15,000 per hour loss
- 4-hour average time to repair
- 1 cable cut per year on average
- $60,000 lost business for 1 cable cut
Incident Management

What are the odds?

• Two devices in series, each with a reliability of 99%, yields a system reliability of 98% \( (0.99 \times 0.99 = 0.9801 = 98.01\%) \)

• Two devices in parallel, each with a reliability of 99%, yields a system reliability of 99.99% \( (1 - (0.01 \times 0.01)) = 0.9999 = 99.99\% \)
Incident Management

What are the odds and what are the consequences?

- **High probability, minimal consequences - Printer/copier breakdown**
- **Medium probability, possible major consequences - Commercial AC power failure**
- **Low probability, major consequences - Fire**
Incident Management

Disaster Recovery Lessons Learned
Incident Management: Lessons Learned

IBM, Sungard Research

• Stress and trauma effects get worse every day for a significant period of time during disaster recovery operations.
• Companies fail to update capacity needs over time.
• Protecting and providing for home and family come first.
Incident Management: Lessons Learned

- Networks were not easy to recover.
- As a result, companies seriously under-estimated the time needed to recover.
- Some of this was due to unavailability of key personnel.
- As the incident winds down it can be difficult and expensive to integrate ad hoc recovery systems into the organization’s production systems.
Incident Management

Business vs. Personal Priorities
Incident Management: Personal Planning

Everyone Needs A Plan: What’s Yours?
Incident Management: Personal Backup

- Phone (backed up?)
- Valuable papers (scanned?)
- Data backup (off site?)
- House (correct and adequate insurance?)
- Internet service (alternatives?)
- Keys (duplicates?)
- Wallet (what’s in it?)
- Medications and eyeglasses (alternative sources?)
- Credit cards (and cash!)
Incident Management: Personal Backup

• **What’s In Your Car?**
  — Flashlight *(fresh/spare batteries?)*
  — Spare tire *(with correct air pressure)*
  — First aid kit *(how old?)*
  — Tools *(at least basic)*
  — Fire extinguisher *(how old?)*
  — Flares?
  — Maps?
  — Blankets? Food? Water?
Incident Management: Planning
Incident Management: Planning

- Decision Tree: What am I dealing with?
- Goals
- Scope
- Incident Management Structure
- Command Control and Communications
Incident Management: Priorities

• Ensure the safety and welfare of employees.

• Outline the chain of command for incident management.

• Control the cost and duration of such an event.
Incident Management: Priorities

- Get Home
- Get Seen
- Get Water
- Get Shelter
- Get Treatment
- Get Safe
- Get Out

Personal/Family Priorities
Incident Management: Priorities

Business Priorities

- Ensure the safety and welfare of employees, visitors and the public
Incident Management: Notifications
Incident Management: Priorities

- Outline the chain of command for the incident
Incident Management: Priorities

Assess damage to facilities
Incident Management: Priorities

Control the cost and duration of the incident
Incident Management: Planning Questions

- What are the threats?
- What are the risks?
- What are the consequences?
- What do I need?
- What do I have?
- Where do I get it?
- Where do I put it?
- When do I need it?
- Who will install and operate it?
## Incident Management: Risk Assessment

### Default Risk Tolerance Matrix

<table>
<thead>
<tr>
<th>Risk Probability</th>
<th>Meaning</th>
<th>Negligible (5)</th>
<th>Minor (4)</th>
<th>Moderate (3)</th>
<th>Major (2)</th>
<th>Catastrophic (1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMPROBABLE (E)</td>
<td>Very unlikely to occur</td>
<td>GREEN</td>
<td>GREEN</td>
<td>GREEN</td>
<td>WHITE</td>
<td>YELLOW</td>
</tr>
<tr>
<td>REMOTE (D)</td>
<td>Unlikely to occur</td>
<td>GREEN</td>
<td>GREEN</td>
<td>WHITE</td>
<td>WHITE</td>
<td>YELLOW</td>
</tr>
<tr>
<td>OCCASIONAL (C)</td>
<td>Roughly even chance of happening</td>
<td>GREEN</td>
<td>WHITE</td>
<td>YELLOW</td>
<td>RED</td>
<td>RED</td>
</tr>
<tr>
<td>PROBABLE (B)</td>
<td>Likely to occur</td>
<td>GREEN</td>
<td>WHITE</td>
<td>YELLOW</td>
<td>RED</td>
<td>RED</td>
</tr>
<tr>
<td>FREQUENT (A)</td>
<td>Very likely to occur</td>
<td>GREEN</td>
<td>WHITE</td>
<td>YELLOW</td>
<td>RED</td>
<td>RED</td>
</tr>
</tbody>
</table>
Incident Management: The Team

- I.T.
- Telecom
- Human Resources
- Facilities Management
- Security
- Finance/Accounting
- Marketing
- Operations
- Manufacturing
- Legal
- Who is (or should be) on your team?
Incident Management: What do I need?

- PCs, laptops, tablets, network hardware, UPS
- Tables, chairs, desks, tents
- Telephone system
- Office supplies, copies, printers, FAX machines
- Portable toilets
- Catering
Incident Management: What do I need?

• Heavy equipment
• Hotels, bus companies
• Cash!
• Bottled water, meals, ready to eat 😊
  • Get to know suppliers before you need them
  • Where do you get sandbags at 3:00 a.m.
  • Who is (or should be) on your team?
Incident Management: Government Agencies

• Don’t forget local, county, state and federal agencies.
• In certain circumstances these agencies may be the only source of materials required for the recovery effort.
  • Get to know them before you need them.
Incident Management: Gap Analysis

• Captures the difference between what we need or would like to have vs. what we have.

• Can be used for creating strategic (not tactical) long-term plans and budgets.

• Helpful to review progress to meeting future requirements.
Incident Management: Priorities or Deadlines

• If you haven’t done it before, it’s R&D.

• Recovery is a sequence of priorities that do not lend themselves to exact timetables.

• Especially at the beginning of an incident, it may be unrealistic to predict when things will get done.

• The majority of the plan is at the mercy of internal and external resources over which you have little or no control.
Incident Management: The Supply Chain

• Do your **suppliers and other stakeholders** have acceptable business continuity plans?

• Should you review their plans?

• Should you be doing business with firms that do not have adequate disaster recovery plans?
Incident Management: Travel

- What about foreign operations?
- Who does the planning?
- How many of your staff could go overseas and for how long?
- Passports?
- What staff members have foreign language skills?
Incident Management

What Could Go Wrong?
Incident Management

Backup Facilities
Incident Management: Backup Sites

• Do you need a hot site, a warm site or a cold site.
• Costs coming down for commercial sites (e.g., Sungard, Iron Mountain)
• More focus on LAN, WAN and Cloud recovery.
• Limit persons authorized to activate disaster recovery facility to avoid “false alarm” activation fees.
Incident Management: Backup Sites

Geospatial Issues

In general, the farther apart, the better if you need to plan for natural disasters like hurricanes, snow storms, tornadoes, power grid outages ...

Locating facilities less than 100 or even 500 miles of each other may not provide adequate protection from natural disasters.

- New York backup up in Chicago
- Los Angeles backup up in Dallas
- Miami backup up in Dallas
Incident Management: What Can Go Wrong?

- Actions of disgruntled employee
- Power and telecom cable cuts, equipment failure
- Strikes
- Hacking including BCS, BMS and BAS systems
- Water damage (leaking roof, sewer backup, sprinkler system, pipe/fitting failure)
- Floods
- Wind damage
- Hurricane: 2012 Sandy ($50+ billion)  2005 Katrina ($108+ billion)
- Fire damage/explosion/hazardous materials
- Solar flares
Incident Management: What Can Go Wrong?

The Metro Section

The New York Times

FRIDAY, DECEMBER 20, 2002

Power Fails for 3 Hours at Plum Island Infectious Disease Lab

By MARC SANTORA

A three-hour power failure at the Plum Island Animal Disease Center last weekend renewed concerns about the safety of the high-security government laboratory while it is being shut down for maintenance, including a five-months strike. The loss of power and failure of all three backup generators raised fears for the first time that the containment of infectious diseases could have been seriously compromised at the laboratory. The center, which is run by the United States Agriculture Department, studies highly infectious animal diseases like foot and mouth disease and African swine fever.

Senator Hillary Rodham Clinton called yesterday for the laboratory to cease all operations until an independent safety review could be conducted.

Scientists familiar with the center said that since the diseases studied on the island are not, for the most part, affect humans, the impact on workers at the center and in residents of the nearby North Fork of Long Island was minimal. Several experts in infectious diseases said, however, that a power failure at such a facility for so long was extraordinarily unusual.

Ken Albeck, a former top Soviet germ warfare official now at George Mason University, said that although he knew of power failures at similar facilities, he did not know of a case in which the power and all the backup generators failed for this long.

"If there was no pathogen in the air, they may not need to quarantine but they need to take steps to be sure there was no contagion," Sandy Hayes, a spokeswoman for the Agriculture Department, said that day after the power failed, safety inspectors rechecked what had happened. "They said they were sure there was no bio-containment breach," she said. She said that all animals were being monitored and that none had shown any signs of problems.

Ms. Hayes said that Plum Island called the Long Island Power Authority on Sunday about 1:30 p.m. reporting that the voltage it

Continued on Page B10
Incident Management: What Can Go Wrong? Why Generators Don’t Start

- Battery failure: lead sulfate buildup, battery charger turned off, lack of maintenance.
- Radiator: coolant leaks, plugged core.
- Air in the fuel system.
- Low coolant temp alarm: block heater failure.
- Controls not in “Auto”: human error.
- Out of fuel: bad fuel gauge, plugged fuel filter, faulty emergency shut-off solenoid.
- High fuel level alarm: thermal expansion of fuel.
- Breaker trip: human error or Automatic Transfer Switch failure.
Incident Management: What Can Go Wrong?

Denied Access

- Police activity, state of emergency, civil unrest, gas leak, HAZMAT
- No damage, but you can’t get into the building.
Incident Management: What Can Go Wrong?
The Cloud Goes Away
Incident Management: What Can Go Wrong?

The Cloud Goes Away
Incident Management: What Can Go Wrong?

Your Secure Off-Site Falls Apart
Incident Management: What Can Go Wrong?
Filnames That Don’t Make Sense

- Filenames that make no sense
  - mtg rpt.docx vs. 101305_sales_by_div.docx

- Using email as a filing cabinet
  - Lack of proper (hardcopy) documentation
  - Lack of configuration management
Incident Management: Planning For

http://www.nucleardarkness.org/nuclear/nuclearexplosionsimulator/
Incident Management: Planning For
Incident Management: Will the plan work?

- Never as planned.
- Some things will always be beyond your control.
  - The plan you make
  - The plan you execute
  - The plan you wish you had executed
- Get creative, make it work.
Incident Management: Critical Success Factors

✓ Luck
✓ Communication
✓ Preparation
✓ Execution
✓ Cooperation
Incident Management: Critical Success Factors

United Airlines Flight 232 / July 19, 1989 / Sioux City, Iowa

What are the odds?
Of having an uncontained compressor blade failure cause the failure of the triply redundant hydraulic system?

1,000,000,000 to 1 (estimated)

As a result, no emergency procedures had ever been created for this failure.
Incident Management: Critical Success Factors

United Airlines Flight 232 / July 19, 1989 / Sioux City, Iowa

What are the odds?
Of keeping the plane in the air for 42 minutes? The first thirteen crews that flew the flight simulator reconstruction of the event were unable to fly the plane to a successful outcome.

• Keeping the plane in the air allowed rescue crews time to arrive and take position.
• Sioux City Airport held worst-case (not most likely) disaster drill the year before the incident.
• Mid-afternoon timeframe allowed the city’s two hospitals and other agencies to hold over day-shift staff.
Incident Management: Critical Success Factors

United Airlines Flight 232 / July 19, 1989 / Sioux City, Iowa

- DC-10 check pilot on-board as passenger.
- No typical summer thunderstorms.
- It was the one day per month when the Air National Guard was on duty at the airport.
- Calm, confident voice of Air Traffic Controller helped aircraft crew focus on immediate tasks.
Incident Management: Critical Success Factors

United Airlines Flight 232 / July 19, 1989 / Sioux City, Iowa

- When Flight 232 touched down:
- it was the same type of aircraft
- on the exact same runway
- at the exact same location
- as the used to create the prior year’s disaster drill.

The only difference was that the drill was based on 150 survivors. Flight 232 had about 200.
Incident Management: Critical Success Factors

United Airlines Flight 232 / July 19, 1989 / Sioux City, Iowa

• When First Officer Bill Records said “I can’t control the airplane” Haynes said he grabbed the control wheel and said “… dumbest thing I’ve ever said: ‘I got it Bill.’ ”

• Capt. Haynes: “The day of ‘I will solve the problem’ is over. Now it’s ‘We will solve the problem.’ ”

• It’s possible the best words you will ever hear anyone say are: “I’ll take over” or “I’m in charge.”
Incident Management: Critical Success Factors

USAir Flight 1549 / January 15, 2009 / New York, NY
Incident Management: Natural Disasters
Incident Management: Natural Disasters

ACCU-WEATHER
RADAR & SATELLITE

RIVER FLOODING

<table>
<thead>
<tr>
<th>RIVER</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASSAIC</td>
<td>FLOODING</td>
</tr>
<tr>
<td>WANAUKE</td>
<td>FLOODING</td>
</tr>
<tr>
<td>RARITAN</td>
<td>FLOODING</td>
</tr>
<tr>
<td>RAMAPO</td>
<td>FLOODING</td>
</tr>
<tr>
<td>ROCKAWAY</td>
<td>FLOODING</td>
</tr>
<tr>
<td>MILLSTONE</td>
<td>FLOODING</td>
</tr>
<tr>
<td>PEQUANNOCK</td>
<td>FLOODING</td>
</tr>
</tbody>
</table>

ACCU-WEATHER
TODAY

50 SOAKING RAINS
Incident Management: Flooding

What Are The Odds?

In 2004 the east coast experienced a 1-in-100-year storm
In 2005 the east coast experienced a 1-in-500-year storm

Remember, odds are calculated based on long-term averages. So it is possible to have multiple rare events occur within a short period of time.
Incident Management: Power Grid Failure

* 1996: 4m people hit by electricity outage across nine states
* 1977: lightning strike leaves New York without power for 25 hours
* 1965: power loss in north-east US and southern Canada hits 30m people
Incident Management: Power Grid Failure

- Stranded commuters spent the night asleep on the street.
- The blackouts caused huge disruption.
- In 1977 shop owners stood guard with baseball bats during bouts of looting.
- The bridges leading out of Manhattan were overrun by crowds.
Incident Management: Telecom Offices

Telecom Central Office Fires
Bell Canada 1999
Deutsche Telecom 1998
Hinsdale, IL 1988
Incident Management: What Could Go Wrong?

THANK YOU FOR CALLING “ON-STAR”... HOW CAN WE HELP YOU?

2017 BICSI CANADIAN CONFERENCE & EXHIBITION
MAY 8-11 • VANCOUVER, BRITISH COLUMBIA, CANADA
Incident Management

Insurance
Incident Management: Insurance

• Some examples of insurable events:
  • Storm/wind damage
  • Flood
  • Fire
  • Loss of commercial AC power
  • Product defects

• Some examples of (typically) non-insurable events:
  • Civil unrest, riots
  • Terrorism
Incident Management: Insurance

One Event or Two?

Why does it matter?

Multiple Occurrences/Deductibles. Was the attack on the World Trade Towers one event or multiple events?

One event, one deductible. Multiple events, multiple deductibles.
Incident Management: Insurance

**Business Interruption Insurance**
- Covers basic and direct losses.
  - Loss of revenue.
  - Payment of operational expenses (e.g. electricity).
  - Payment of (some) salaries.
  - Typically has 48-hour waiting period.
  - Typically provides coverage for 30 days of loss.

**Extended Period of Indemnity**
- Provides basic coverage beyond 30 days.

**Extended Coverage**
- Pays for losses after repairs are done and pre-event revenue levels are restored.
Incident Management: Insurance

Extra Expense Coverage
- Pays for restoring business records, legal expenses, etc. not directly related to the event.

Contingent Coverage
- Provides coverage for losses caused by others (e.g. fire at a supplier’s factory).

Coinsurance
- Insured pays a share of loss if the loss is greater than the amount of the insurance coverage.

Ordinary Payroll Coverage
- Excludes non-executive and management payrolls.
Incident Management: Insurance

Under-insuring may impair coverage. For example, if the loss is $10 million and the insurance coverage is $8 million, the insurance company may only be obligated to pay 80% of the coverage amount or $6.4 million.

The theory is that the insured was trying to avoid buying the proper amount of insurance to reduce its premium costs.
Incident Management: Insurance

• **Fiction:** 80% of all business that have a serious business interruption go out of business within 1 year (or some variation of this theme).

• **Fact:** This is a statistic from many, many years ago that is still being repeated today with one word left out. The missing word from the original statement is **under-insured**.
Incident Management

Incident Analysis

Data Collection & Reporting
Incident Management: Incident Analysis

• **Why?** To collect incident information in a uniform manner so that it may be analyzed and presented to senior management.

• **Goal?** To help justify the time and expense required to create, maintain and test the Business Continuity Plan.

• **Benefit?** To demonstrate that analysis of past incidents leads to corrective actions that mitigate future incidents.
Incident Management: Incident Analysis

- **Category A Event**
  An event requiring the activation of the off-site recovery facility.

- **Category B-1 Event**
  An event resulting in the major disruption of normal business functions for one or more business units for more than 24 hours:
  - (1) requiring the expenditure of significant funds; or
  - (2) incurring significant regulatory fine or penalties, but
  - (3) not requiring the activation of the off-site recovery center.
Incident Management: Incident Analysis

• **Category B-2 Event**
  An event resulting in the major disruption of normal business function for one or more business units for more than 24 hours:
  • (1) not requiring the expenditure of significant funds;
  • (2) not incurring significant regulatory fines or penalties; and
  • (3) not requiring the activation of the off-site recovery center.
Incident Management: Incident Analysis

• **Category C-1 Event**
  An event resulting in the major disruption of the normal business function of one or more business units for less than 24 hours incurring significant regulatory fine or penalties.

• **Category C-2 Event**
  An event resulting in the major disruption of the normal business function of one or more business units for less than 24 hours that does not incur significant regulatory fine or penalties.
Incident Management: Incident Analysis

- **Category D Event**
  An event resulting in the minor disruption of normal business functions which can be restored using internal resources.

- **Category E Event**
  All other events not classified above.
Incident Management: Incident Analysis

Critical Recovery Team Information

1. Date and time incident was discovered.
2. Actual or estimated date and time incident started.
3. Which person or agency first discovered the incident?
4. Who was the first employee notified of the incident?
5. If applicable, which public safety agency is in-charge?
6. Time business recovery team notified.
7. Where should the recovery team meet? At incident or alternate site?
Incident Management: Incident Analysis

Critical Recovery Team Information

1. Injured or missing personnel.
2. Damage to building.
3. Damage to business systems.
4. Will physical access to building be delayed?
Incident Management

Legal Issues
Incident Management: Legal Issues

Some industries are legally required to have business continuity plans (e.g. healthcare, financial) with statutory or regulatory periodic reviews.

- **Sarbanes-Oxley Act of 2002 Section 404** (ensuring data integrity and availability for compliance and attestation).
- **Health Insurance Portability and Accountability Act (HIPAA) of 1996** (information privacy).
- **Gramm-Leach Bliley Act (GLBA) of 1999** (information privacy).
Incident Management: Legal Issues

• Directors and officers may be personally liable for failing to adequately protect corporate assets.
• Create Board of Directors Approval Form
• Disaster recovery plan is part of protecting corporate assets.
• Board of Directors should pass formal motion reviewing and recognizing the disaster recovery plan.
Incident Management: Legal Issues

BOARD OF DIRECTORS APPROVAL
Approval and Authority of the Board

After careful review and deliberation, we, the Board of Directors, do hereby approve this Business Recovery Plan for use as described herein. Furthermore, we do hereby vest full responsibility and authority for the execution of this plan in the members of the business recovery team.

______________________________
Chairman of the Board

______________________________
Date
Incident Management: General Principles

Managing incidents becomes rapidly more difficult as the number of nodes increases.

<table>
<thead>
<tr>
<th>Number of Components</th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Possible Connections</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>6</td>
<td>28</td>
<td>66</td>
</tr>
</tbody>
</table>

2017 BICSI CANADIAN CONFERENCE & EXHIBITION
MAY 8-11 • VANCOUVER, BRITISH COLUMBIA, CANADA
Incident Management: General Principles

• A person’s short-term memory can hold only five to nine pieces of data before new data replaces the old.

• Document it
• Write it down
• Draw it

• Remember, it’s not just what you know but how effectively you can communicate it to your replacement and team that counts.
Incident Management: General Principles

- Every incident must have a designated *coordinator, manager or commander*.

- All incident command functions must be performed. At minor incidents one person may perform all functions.

- Costs associated with an incident should be charged to a *separate and distinct accounting code* to facilitate insurance reimbursement claims.
Incident Management: Insurance

• Check for “No damage, no coverage” clause.

• Consult with insurance carrier for ideas and discounts.

• The owner is responsible for preventing any additional damage after the initial incident (e.g., freezing of pipes after a fire; theft because the site was not secured after an incident).
Incident Management: Public Relations

• Incidents large enough to attract the news media will require that only the officially designated Public Information Officer (PIO) speak for the organization.

• NOTE: You can go “Off the record”, but if you say it, be prepared to have it repeated.

• For some reporters, nothing is “Off the record”.
Incident Management

Notifying the Team

Who’s Available When?
or
Where in the World is My DR Team?
Incident Management: Staffing

Mapping and Geographic Information Systems (GIS)

- Get staff addresses including home and vacation home
- Aggregate by region, neighborhood, ZIP code, etc.
- Map locations
- Determine locations for pick up by public or charter services
Incident Management: Staffing
Incident Management: Controlling Response

Control The Response

• Understand how you will use the response team.

• If you have no defined task for the individual they should report to a staging area, not to the recovery operations area.

• The staging area must have a personnel tracking system in place (on-site, resting, off-site, dismissed)
Incident Management: Controlling Response

- Anyone who has completed their assignment should return to the staging area.

- **At all costs, prevent free-lancing.** It can be dangerous and costly to the individual and the organization in terms of both time and money.
Incident Management: Controlling Response

- Establish a centralized phone, email, text response message system
- Identify the caller (e.g. employee ID number)
- Tell them when and where to report and how long they will be on site
- Obtain estimate of how long it will take the person to respond
- Allow for different time zones and international date line, if required.
Incident Management: Minor Incident

Broken Copier/Printer

• How often does it occur?
• When does it occur?
• Consequences?
• Response strategy?
• Response tactic? Repair, replace, preventive maintenance, change service company
Incident Management: Minor Incident

Communicate Status

• Place sign on copier
  • Copier Out of Service
  • Repair Called at 11:15 AM June 10
  • Repairs should be completed by 3 PM
  • Next update 2:00 p.m.
  • Contact: Ron Smith extension 209

THE COPIER ISN'T BROKEN.
I JUST PUT THAT SIGN THERE SO I DON'T HAVE TO WAIT IN LINE...
Incident Management: Major Incident

- Electrical system failure
- Frequency?
- Time-of-Day?
- Consequences?
- Recovery Team?
- Remedy: Implement recovery plan
Incident Management: Major Incident

PRIORITIES
1. Establish Command Center
2. Identify who is in charge of what.
   
   It doesn’t need to be fancy - butcher paper taped to the walls will do!
3. Assign people to tasks.
4. Collect and analyze data (e.g. is it a power company problem, damaged company-owned equipment or both?).
5. Notify and direct employees as appropriate.
COMMUNICATE STATUS!

- Text, email, update Web site, 800#, radio announcements, ....
- Decide if off-site location will be needed.
- Use Geographic Information Systems (GIS) to optimize car pools and bus routes.
  - (What if you can’t use planes, trains or cars?)
- Have staff retrieve disaster plans.
- Keep everyone informed.
  - Update Web site
  - Issue press release
Incident Management

War Rooms
Command Centers
Network Operations Centers
Incident Management: Command Centers

9/11
NYC Office of Emergency Management
23rd Floor, 7 WTC
Incident Management: Command Centers

Post 9/11
Cadman Plaza, Brooklyn, NY
Incident Management: Command Centers
Incident Management: Command Centers
Incident Management: Command Centers

When staffing a command center, remind everyone to bring:
- one-week supply of clothes
- toiletries, contact lens supplies, etc.
- medications
- cell phones and
- and make arrangements for taking care of their home, plants, pets, mail, paying bills and newspaper delivery.
Incident Management: Command Centers

Note: Given the conditions in which people will be working, it would be good practice to obtain the names of, and contact information for, relatives, personal physicians, etc.
Incident Management: Command Centers

- The services of a professional conference or event planner may be helpful in locating a command center or recovery site.

- Don’t forget to keep a list of business catering firms in the recovery kit. Fast food and pizza will keep the team going for just so long.

- Depending on the time of year, schools and colleges may be available to have dorm space and conference rooms available.
Provide concierge service to free up staff.
To help its employees recover from natural disasters companies have found that providing classes on making repairs, rehabilitating appliances, and obtaining disaster relief aid (as well as providing the names of reputable contractors) reduced the average time employees were away from work.
Incident Management: Planning Goals

Create a **flexible** set of responses to events that may interfere with normal business activities based on:

- (1) the **economic impact** of the event(s)
- (2) the organization’s approach to **risk management**
- (3) the **budget** available.
Incident Management: Planning Goals

A practical plan is an intelligent trade-off of:

• (1) time,

• (2) budget, and

• (3) resources.
Incident Management: Planning Goals

Even if there is a plan, how do you measure the quality of the plan?

Getting it on paper doesn’t mean it will work!
Incident Management: Planning Goals

Now consider that the Disaster Recovery Preparedness Council’s 2015 annual report claims that only 33% of survey participants test their DR Plan – and 65% of those who do, *fail* their own test.

In 27% of the firms, non-I.T. managers were not part of the disaster recovery process.
Incident Management: Planning

4. 54% of companies report they have experienced downtime from a single event, lasting more than 8 hours. *Eight hours of continuous downtime is full day of work.* Here is a downtime calculator so that you can see what that translates to in dollars and cents.

5. 75% of all downtime is reported to be due to a power outage. Hardware and human errors round up the top three. *In other words, even if you are not worried about safeguarding your business from a natural disaster, you still need to safeguard your business.*

6. 1 in 3 organizations have reported being hit by a virus or a malware attack within the last 5 years. *With malware on the rise, the numbers are only expected to rise, which is why cyber-education and protection are so important.*

7. 2 in 5 companies still do not have a documented disaster recovery plan, and over a quarter admit to rarely to never testing them. *Yikes. I know that if you’re reading this, you must have a disaster recovery plan in place, which is tested and adapted regularly!*

8. Over one third of IT professionals are frustrated with business continuity solutions, citing they are too difficult to use. *Business continuity has evolved so much over the last few years. Not all BCDR technology is confusing: we promise.*
Incident Management

The Recovery Kit
Things To Be Stored Off-Site
Incident Management

Staff should not keep resources at home or in the car. Use a professional records management firm for off-site resource storage. They can deliver to your recover site.

Do not depend on ECTAM.

Employee’s Chevy Truck Access Method
Incident Management: Recovery Kit

• Copies of the Business Recovery Plan
• Building floor plans with the location of mission-critical equipment marked for salvage operations
• Data and network backup
• If tape backup, spare tape transport system
• Original software media
• Keys to company facilities and vehicles
Incident Management: Recovery Kit

- Flashlights
- Cameras
- Hard hats
- Protective overalls (bunny suits)
- Wire Cutters
- Cable and FiOS adapters
Incident Management: Recovery Kit

- Command Vests (Finance, Telecom, Logistics ...)
- Office and planning supplies: flip-chart paper, pads, pens, tape grease pencils, Post Its, etc.
- Fire Codes (system passwords)
- Industrial handheld radios with GPS
- Ceiling signs (to identify team functions: finance, telecom, logistics ...)
- Purchase orders with unique numbering designating disaster recovery operations
Incident Management: Recovery Kit

Each business unit must analyze their specific business processes (e.g. high volume invoice printing) and determine what specialized equipment, business forms, supplies, etc. must be stored off-site.
Incident Management

Security & Access Control
Incident Management: Security/Access

After securing the area – control access!

- Good practice at all times, but even more so when there is confusion and opportunity for theft by clean-up and construction crews.
- Track visitors and know where they are.
- Limit liability claims:
  - “I worked on that job .....”
Incident Management: Security/Access

Use self-expiring badges
• 2 hour, 1 day, 1 week and 1 month (standard)
• Pre-printed or print-on-demand
• Use different styles and shapes to identify function
• Use log sheets to track badges; be especially careful of “lost” and “void” badges
Incident Management: Security/Access

One source of security tape and self-expiring visitor badges is:
Temtec, Inc. (Brady)
PO Box 823
20 Thompson Rd.
Branford, CT 06405
800-628-0022
www.tempbadge.com
Incident Management

Password Management
Incident Management: Password Management

• Bypassing Ad Hoc User Passwords
• Bypassing Network Administrator Passwords
• The “Fire Code” Password System
• Challenge and Response Systems
Incident Management: Password Management

• In an emergency, the need may exist to bypass passwords

• Software is available to bypass passwords in many application software packages (e.g. Microsoft Word, Excel) and Network Operating Systems (e.g. Windows Server).
Incident Management

The Fire Code Password Control Method
Incident Management: Fire Code

Features

• Secure method of documenting access codes.
• Depends on “trusted administrator”.
• Allows access when critical personnel are not available.
• Can be used in normal business functions where ad hoc access to secure systems is needed.
Incident Management: Fire Code

Implementation

• Place password on blank piece of paper
• Put this paper in an envelope
• Administrator places random number on outside of envelope
• Seal envelope with security tape
• Fill out form describing system on separate piece of paper (password does not appear on this paper)
Incident Management: Fire Code

- Administrator places random number on this sheet
- Administrator creates cross-reference between numbers
- Cross-reference is stored in a very secure place
- Envelope and system description sheets filed
Incident Management

Locating & Tagging
Mission-Critical Equipment
Incident Management: Tag Equipment

Why? To facilitate the recovery of mission-critical equipment.

How? Tag all items considered mission-critical with 3” diameter fluorescent (e.g. orange, red, green) stickers to aid in the locating of these items. The location of mission-critical items must be noted on the building’s floor plans. Keep copies of the floor plans on-site and off-site.
Incident Management: Salvage

Note:
When time is critical, cut, don’t disconnect, data cables that are mechanically fastened to the equipment. If salvage time is limited (“You have 15 minutes to go into the building and get what you want”), don’t waste time salvaging easily replaced items such as monitors, cables, and keyboards, but rather concentrate of retrieving as many PCs and servers as possible.

NEVER cut a power cord. Even if commercial AC power is disconnected from the building, power from a UPS or standby generator may be present.
Incident Management

Fireproof Digital Medium Storage
Incident Management: Records Storage

• Conventional fire proof safes absorb moisture and then create a steam atmosphere within the enclosure when exposed to fire conditions (400+ degrees F).
• This is an unsafe condition for magnetic materials like backup tapes or legacy mechanical hard drives.
• ANSI/NFPA Standard #75 states temperatures above 120° F are damaging to magnetic materials.
• BUT
• NFPA Standard 232 for Protection of Records, Appendix A states a maximum of 150° F and 85% humidity is OK for magnetic materials.
Incident Management

All Things Come To An End
Including Disasters
Incident Management: Disengaging

All Incidents Will Eventually End

• How do you phase out of recovery mode?
• Planning for how to return to normal operations is often forgotten.

Winding down a recovery operation will very likely to be much more complex than activating the plan.
Incident Management

Human Factors
Incident Management: Human Factors

- The recovery team will be made up of many different types of personalities. Unfortunately, some of them will be disruptive to the recovery process.
- Match tasks with personalities.
- Reassign people if required.
- If that can’t be done, give serious consideration to removing them from the recovery team.
Incident Management: Human Factors

- People are human.
- Adrenaline lasts only so long.
- Enforce shift changes as soon as you can.
- Make sure information exchange at shift change briefing is comprehensive.
- Make sure recovery team takes breaks for sleep and meals.
- Watch out for Superman.
Incident Management

The Incident Decision Tree
Incident Management: Event Decision Tree

Incident Discovery Action

- After Hours
  - Notify Management
    - Call appropriate managers
      - Describe: situation, who is at the location where to report.
- During Business Hours
  - Need to Evacuate Bldg?
    - If Yes, Select Assembly Location.
Incident Management: Event Decision Tree

AFTER HOURS

Notify Management

Describe: situation, who is at the location, where to report.

Notify Employees

When, where and if to report.
Incident Management: Event Decision Tree

Need to Evacuate Building?
If yes, select assembly location.

Alternate Assembly Point
To be used if building is not accessible.
All employees report here

Assign Incident Manager
Take responsibility for incident until relieved.

Take Head-Count
Injury assessment Account for all personnel including visitor and contractors.

Missing Personnel?
Notify emergency Workers. Notify business recover team members. Notify family.

Delayed Return to Building?
Release employees and obtain contact phone numbers.

Local assembly point
Used if building is accessible.
All employees report here
Incident Management: Event Decision Tree

Delayed Return to Building
Release employees and obtain contact phone numbers.

Bus. Recover Team Setup
Sign-In. Assign to positions in recovery Organizational Chart.

Off-Site Storage Site
Pick up recovery kit

Initial Assessment
Unable to continue business as usual?

Employee Notification

Agency Notification
Notify business partners, postal service, etc.

Employee Communications
Announcements on predetermined AM/FM radio stations.
Incident Management: Event Decision Tree

- Employee Communications
  - Announcements on predetermined AM/FM radio stations.
- Fill Recovery Team Pos.
  - Assign arriving business recovery team members to positions in recovery organizational chart
- Activate Recovery Facility?
  - Use Off-site recovery facility?
    - YES
      - Divide recover team into on-site and off-site teams.
    - NO
      - Select on-site recovery facilities.
- Get All Recovery Items
  - Obtain all items stored off-site to implement full-scale recovery program.
- Reroute Telecom Ckts
  - Switch to alternate routing paths.
Incident Management

Basic Incident Command Structure
Incident Management: Basic Cmd Structure
Incident Management

Complex Incident Command Structure
Incident Management: Complex Cmd Structure

Keep recovery networks separate from the organization’s networks except as required for testing.
Incident Management: Complex Cmd Structure

- Incident Mgmt. Team
  - Sets Objectives
- Administrative Support
- Off-Site Team
- Operations
- Planning
- Logistics
- Finance
- Communications
Incident Management: Review

• Create a wide range of recovery scenarios.
• Always designate an incident manager.
• Create *functional* checklists.
• Create a pool of DR team candidates.
• Identify mission-critical equipment with fluorescent stickers.
• Note location of critical equipment on blueprints
  • Store the prints off site.
Incident Management: Resources

NFPA Standard 1600
2016 Edition
1 Batterymarch Park
Quincy, MA  02169-7471
(617) 770-3000
www.nfpa.org
Free PDF download
Incident Management: To Learn More

NFPA Standard 1620
2015 Edition
1 Batterymarch Park
Quincy, MA 02169-7471
(617) 770-3000
www.nfpa.org
Incident Management: To Learn More

Disaster Resource Guide
PO Box 15243
Santa Ana, CA 92735
(714) 558-8940
www.disaster-resource.com
Incident Management: To Learn More

Disaster Recovery Journal
1862 Old Lemay Ferry
Arnold, MO 63010
(636) 282-5800
www.drj.com
Incident Management: To Learn More

**Disaster Recovery Planning**
Author: Jon Toigo
Publisher: Prentice Hall PTR
512 Pages

Dated, but the basics are still relevant.
Incident Management: To Learn More

Disaster & Recovery Planning
Author: Joseph F. Gustin
Publisher: Fairmont Press
ISBN: 978-1482215670
350 Pages
Incident Management: To Learn More

Author: David Casavant
Publisher: Government Institutes (2003)
ISBN: 0-8658-7843-9
308 Pages
Incident Management: To Learn More

Rothstein Publishing
4 Arapaho Road
Brookfield, CT 06804
203-740-7400
www.rothstein.com

Covers all aspects of disaster and business recovery including links to other resources and industry events.
Incident Management: To Learn More

Emergency Management Magazine
www.emergencymgmt.com
Incident Management: To Learn More

Continuity Magazine
www.thebci.org
Incident Management: To Learn More

Security Magazine
www.securitymagazine.com
Incident Management: To Learn More

Incident Management: Certification

Int. Assoc. Emergency Managers
201 Park Washington Ct
Falls Church, VA 22046
(703) 538-1795
www.iaem.com
Incident Management

Ernest Schirmer, Senior Associate
WSP | Parsons Brinckerhoff
One Penn Plaza, 250 West 34th Street
New York, NY 10119
212-951-2835
ernest.schirmer@wspgroup.com