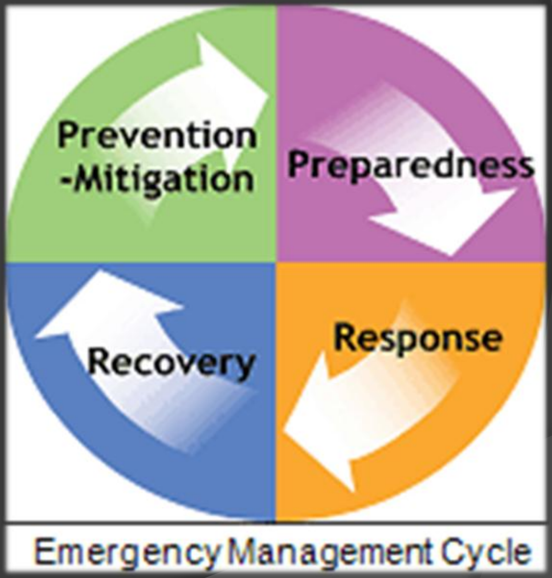
THE ESSENTIALS OF BUSINESS CONTINUITY

Christine Herndon
Herndon Solutions Group
January 17, 2013

Why Plan?

- Mitigate/prevent the incident
- Prepare for an incident
- Respond to an incident
- Recover from an incident



"Prepare for the Worst…Hope for the Best!"

The “Facts”

- 40% of all companies hit by a disaster go out of business
- 93% of companies that experience significant data loss are out of business within five years
- 8 out of 10 businesses are not prepared for a disaster

What is a disaster?

"A disaster can be as mundane as a hot cup of coffee spilled on a computer or air conditioners breaking down causing computer and server failures…"

The “Incidents”

- Natural
- Technological
- Loss of Personnel
- Workplace Violence
- Terrorism

What do we do?

- Identify and evaluate the risk
  - Assess the probability
  - Determine the consequence
- Decide what level of risk you are willing to accept
- Manage the risk/threat without impacting your day-to-day activities
  - Mitigate the risk
  - Plan for response and recovery operations

How do we do it?

1. Management Buy-In
2. Identify Critical Functions and Supporting Systems and Personnel
3. Establish a Crisis Management Team (CMT)
4. Develop an Effective Means of Communication
5. Write the Plan
6. Practice, Practice, Practice!

Where Do I Start?

- Ask the hard questions? What would you do if….
- Identify your critical functions
- Determine your highest risk
- Implement short-term and plan for long-term mitigation measures
- Prepare a "plan" to fully complete your business impact assessment (BIA)/risk assessment, and ultimately prepare your business continuity plan (BCP)

Step 1: Business Impact Analysis (BIA)

- What are your essential functions?
- What products or services do you provide?
- What operational and administrative functions/processes are required to execute your mission?
- What facilities or equipment are needed?
- What records are needed?
- Are their regulatory requirements?
- What do vendors provide?
- What personnel are required?

Step 1

Mission Essential (Critical) Assets

- Servers
- Desktops/laptops
- Printers/scanners
- Other documents
- Phones
- Physical office space
- Standard office supplies
- Personnel
- Food/Water

Step 1

Recovery Time and Point Objectives

- Recovery Time Objective
  - What is your maximum acceptable downtime before your business is “negatively” impacted?
  - What is the maximum acceptable downtime for each essential function identified? –or- How much time is the minimum time to have each function resumed?
- Recovery Point Objective
  - What is the acceptable amount of data loss?

Step 1

BIA “Final”

- Identified financial impact per day if lose any given essential function/service
- Identified business processes and flow for each department
- Initiated plan to document department processes
- Identified critical records required by the department
- Identified any regulatory requirements
- Evaluated the operational impacts to the company if that department was “down”

Step 2: Hazard Assessment

- Identify the hazards using an ALL HAZARDS APPROACH

Hazard	Probability	Human Impact	Property Impact	Business Impact	TOTAL
		IMPACT			

- Assess the Probability
- Determine the impact (consequence)
- Ex. ranking (1 – low, 2 – medium, 3 – high)

Step 2

What is the impact if…..

- You lose power for an extended period of time
- A utility line is cut
- Your office is subject to a fire or flood
- A snow storm shuts down a major throughway to the office
- You lose a significant portion of your workforce
- A key staff member is in an accident
- An email delivered malicious software/malware to the domain
- A failed operation system or software update

Now what?

- At this point, you have completed your BIA (at least to some degree) and you have an understanding of your essential functions and potential areas of concern for those to continue operation in the event of a disruption
- You have identified and ranked your risks leaving you with a mechanism to prioritize the most probable events as related to the impacts on the business
- Now you plan on how to respond, right? NO!

Step 3: Mitigate!

- Mitigation, or prevention, is the foundation for business continuity planning
- Instead of focusing on recovering, the context has changed to "not going down at all"

HARDIN
"We've considered every potential risk except the risks of avoiding all risks."

Benefits of Mitigation

- Tampa Bay Planning Council states the true cost-effective benefits from mitigation are as follows:
  1. Increased life safety for employees and customers
  2. Reduced down-time in production
  3. Protected information systems
  4. Reduced damages to facilities and nonstructural components
  5. Reduced damages to non-vital equipment
  6. Enhanced insurance coverage or reduced insurance deductibles

Mitigate – Human Resources

- Awareness and reporting
  - Reduction in job productivity
  - History of violence
  - Stress in employee’s personal life
- Training
  - Roles/responsibilities in emergency situation
  - Emergency management team with CPR/defibrillator training requirements
  - Information about hazards in your workplace
  - Evacuation procedures
  - Location of emergency equipment

Mitigate – Human Resources (cont'd)

- Employee Preparedness
  - Educate about home and family preparedness
  - Contact information
  - Dependent care
- Internal/External Communications
  - Internal phone tree
  - How communicate with customers?
    - Onsite PBX?
    - Can you forward your phones?
    - Can you retrieve office voicemail remotely

Mitigate – Infrastructure

- Security
  - Mail, visitors, and deliveries
  - Restricting access (e.g., fence, access cards, etc)
  - Surveillance/security cameras
- Flood/major leak
  - Determine if in flood prone area
  - Check for window, roof, or plumbing leaks
  - Regular HVAC services

Mitigate – Infrastructure (cont’d)

- Fire
  - Fire resistant (or at least increased) building materials
  - Fire suppression system
  - On-site fire fighting equipment
  - Ensure detection system working (including alarms)
  - Evacuation plan is posted and tested

Mitigate – Data

- According to the Strategic Research Corporation, primary causes of data loss are as follows:
  1. Hardware system – 44%
  2. Human error – 32%
  3. Software – 14%
  4. Virus – 7%
  5. Natural disaster – 3%

Mitigate – Data Storage

- Where are your servers stored?
  - On the floor?
  - In a rack?
  - In a fire and environment controlled room?
- Hard copy documents
  - Hard copies in secure, fire proof safes
  - Not only technical documents, but any other network/software information
- Tapes….
  - If using tapes, store in fire proof AND magnetic proof safe

Mitigate – Data Backup

- System software (operating and applications)
- Electronic files (briefs, arbitrations, research, etc)
- Establishing a data backup schedule
  - Determine frequency of data change
  - Schedule backups using a reliable backup mechanism (daily, weekly, monthly, and bi-annually)
- Backup storage location
  - On-site
  - At least two duplicate off-site
- TEST YOUR BACKUP MECHANISM!!!

Mitigate – Data Backup (Example)

“Yes of course they had backups, the assistant manager had a garage full of tapes. However, the problem was that there was no machine in the world that could restore the tapes, the VAX machines were so ancient there was not a compatible machine anywhere.”

http://www.computerperformance.co.uk/w2k3/disaster_recovery_restore.htm

Mitigate – Insurance

- Property insurance
- Business liability
- Business interruption
- Flood insurance
- Commercial auto
- Workmen’s compensation
- Errors and omissions
- Umbrella
- Specialized insurance, if appropriate

Step 4: Write The “Plan”

1. Strategic Plan (i.e., management support, goals, and objectives)
2. Emergency Operations/Response
   - How you will respond to an emergency
   - Organizational charts with lines of authority and roles/responsibilities
   - Use checklists and other tools
3. Mitigation Strategy (include short- and long-term mitigation strategies)

The "Plan"

4. Recovery Strategy
   - Identify immediate, short-, and long-term priorities
     - ○ Leverage the results of the BIA to identify critical personnel for each essential function
     - ○ Restore services
     - ○ Payroll and cash advance, if applicable
     - ○ Flexible, reduced hours, telecommute

DILBERT
SCOTT ADAMS
I CAN'T LET YOU TELECOMMUTE BECAUSE THEN I WOULDN'T BE ABLE TO MANAGE YOU.
E-mail: SCOTTADAMS@AOL.COM
YOU'RE MANAGING ME RIGHT NOW, AND ALL IT'S DOING IS PREVENTING ME FROM WORKING.
AND YOUR POINT WOULD BE...?
JUST BEYOND YOUR GRASP.

The "Management System"

- The Business Continuity Management System (BCMS) encompasses all of the above
  - Set of preparedness concepts and principles for an ALL HAZARDS approach
  - Scalable
  - Dynamic
  - Adaptable
  - On-going
- Commitment and Buy-In

Tips for a Successful BCMS

- **Commitment!!!!**
- Perform table top exercises (TTX)
- TTX should focus on a probable scenario
- Prepare an After Action Report to summarize the results of the TTX
- Implement the lessons learned into the BCP
- Conduct a TTX at least once per year
- Update the BCP at least once per year (usually in concert with the TTX)
- **Redundancy and commitment!**

Common Pitfalls

- Lack of management support
- Complacency
- Not updating a BIA
- Only focused on information systems
- No training on the BCP or TTX’s
- Poor communication plan (or call tree) both internally (employees, investors, etc) and externally (customers)
- Insurance – BCP must address replacement costs

Group Exercise

1. How can you get management buy-in?
2. What are some critical functions of your firm and systems/personnel that support them?
3. How can you motivate/encourage your staff to work during/following a disaster?
4. What are your current options to communicate with staff and clients? What are the pros/cons of each?

Practice!

- CMT provides an overview to all firm staff
- CMT department/functional leads provide specific orientation and exercises for staff
- CMT administers a firm-wide exercise
- CMT meets quarterly to conduct a tabletop exercise
- CMT administers a firm-wide exercise at least annually

Use Your Resources!

- Your peers can be your best asset and include not only those within your business but also your “neighbors” in which you share building space
- Utilize existing resources, such as the Disaster Recovery Journal
- Maintain open/active communication lines with industry organizations
- Participate in local, industry focused groups

Conclusion

- An industry “driver” will always surface
- Key is to not fall victim to the complacency but maintain a level of awareness and preparation to ensure business resiliency, regardless of the current threat, and maintain a culture of redundancy, commitment, and adaptability
- Your management system, including your plan, will not be prepared or instituted “overnight”
- Training is key to the success of your program, as without training, it’s worthless

Questions

Christine Herndon

President/COO

Herndon Solutions Group

O: 866.487.3895

C: 702.271.4673

christine.herndon@herndon-group.com

www.herndon-group.com