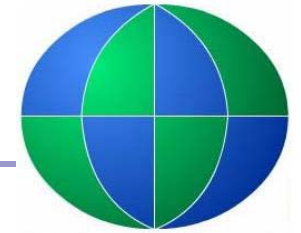


# *Business Continuity Planning*

---



## Fundamentals of Business Continuity Planning

George Washington University  
The Dulles Area Transportation Association

March 31, 2010

By: Gaston Boisson, CBCP, MBCI

# *Overview*

---



- Introduction to Business Continuity
- 2 Case Studies
- 10 steps to an actionable Business Continuity Plan
- 10 steps to start teleworking!

# *What are Business Continuity Plans?*

---



Business Continuity Plans (**BCPs**) are plans to mitigate the risk of losing key operational capacity from disruptive events.

# *Why Plan?*

---



- Respond effectively to disruptive events
- Protect people, systems, and resources
- Sustain operational capability and capacity
- Ensure effective transit capacity during and after disruptive events
- Ensure continued inter/intra state commerce
- Protect business outcomes
- Compliance with NSPD 51/HSPD 20 – National
- Compliance with CGC 1 – State and Local

## *Case Study 1: Nokia Vs. Ericsson*

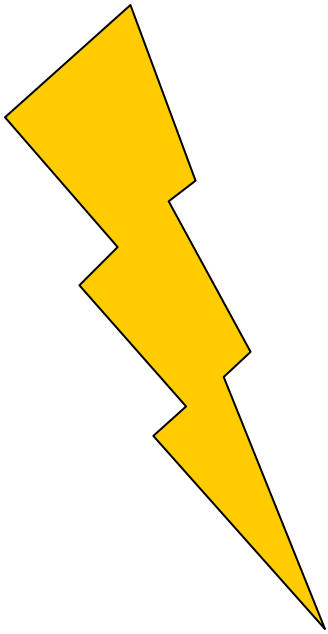
---



- Nokia - international provider of cell phones (Finland)
- L M Ericsson - international provider of cell phones (Sweden)
- Phillips Electronics - manufacturer of cell phone microchips (Holland)

# Event

---



- Albuquerque, NM: Friday, March 17, 2000, 8 pm.
- Lightning bolt hits electric power line, causes a fire in Phillips Electronics Fabrication Plant No. 22.
- Fire is suppressed in 10 minutes.
- Phillips engineers conclude that cleanup will take a week, possibly more.

# *Response and Impact*

---

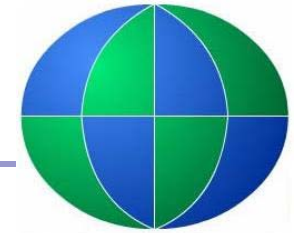


## ■ Nokia

- Cell phone president alerted immediately
- Offered to send Nokia engineers from their Dallas office to Albuquerque
- Daily calls to Phillips
- CEO and cell phone President go to Holland, meet with CEO of Phillips Electronics
- Demand all Phillips production capacity world wide that can process needed chips
- Initiate re-design of chips
- Able to restore production capacity first

# *Response & Impact*

---



## ■ Ericsson

- Procurement staff waited on update calls from Phillips
- Days later staff informs head of mobile phone division that a fire had occurred, and plant wouldn't be up for several weeks
- Looking for replacement chip fabrication capacity, can't find any
- Nokia "got there first"
- Sales are lost

## *Case Study 2: Cantor Fitzgerald*

---



- Two thirds of its entire workforce (658 employees) perished on 9/11
- CEO, whose brother died in WTC Tower Collapse, vowed to keep the company alive
- Difficult decisions on if/how to move forward
- Made decision to spend heavily on supporting the relatives of lost employees
- Resumed operations in 1 week with virtually no data losses
- Within 3 years realizing positive growth

## *Some Fact(oid)s*

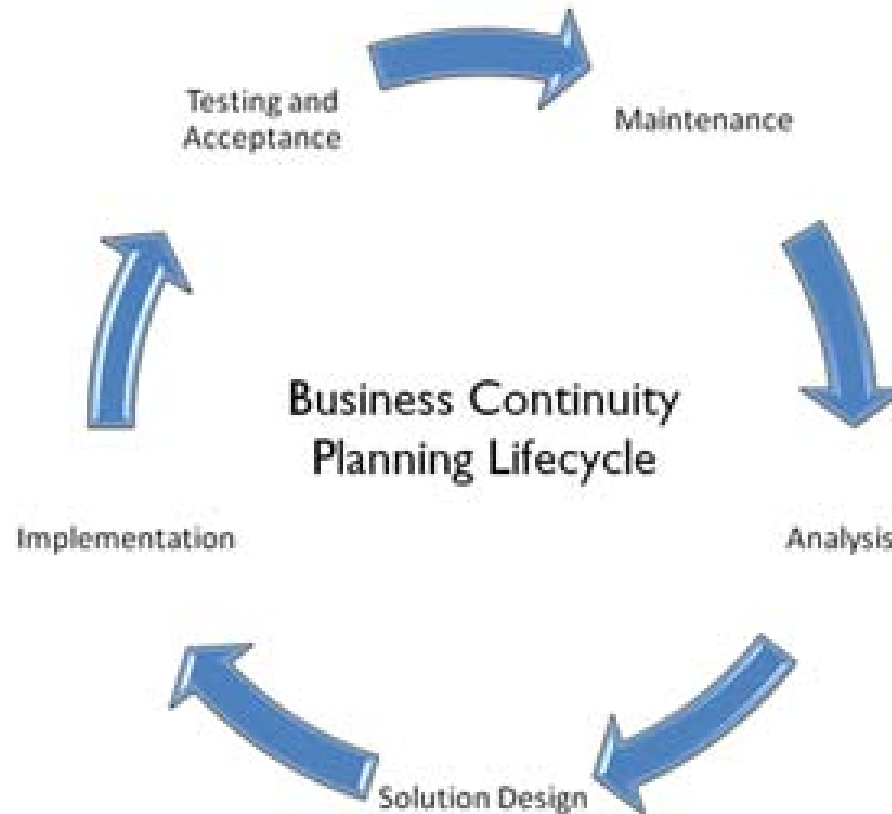
---



- In 2002, Gartner reported that 40 percent of small to midsize businesses that suffer a sudden misfortune will go out of business in 5 years
- Even in 2010, few companies are prepared to deal with disruptive events
- A recent study by Harvard's School of Public Health found that just 1/3 of businesses felt they could sustain operations if 50 percent of their workforce was out for 2 weeks
- DHS Estimates the worker absenteeism could reach 50% for an extended period in the event of an influenza pandemic
- Telework as a continuity strategy is critical!

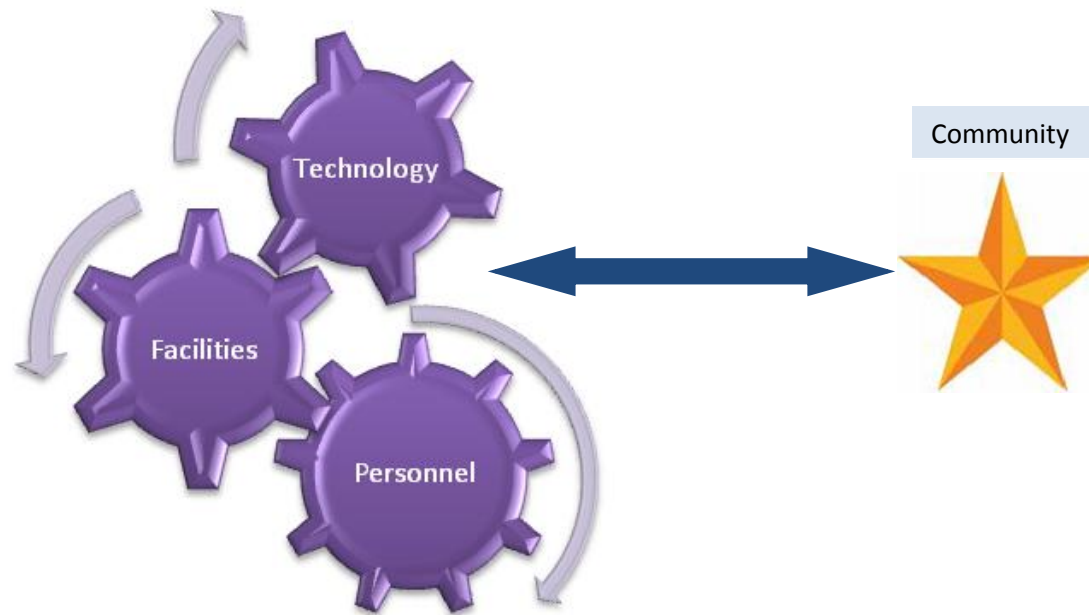
# *BCP Development Cycle*

---



# *What Do We Plan For?*

---



# *Key BCP Development Actions*

---



- Risk Assessment
- Business Impact Analysis
- Business Continuity Strategy Development
- Vetting with Management
- Business Continuity Plan Development
- Rollout of Training, Testing, & Awareness Program
- Implementation of Maintenance Strategy

# *BCP Planning Steps*

---



## **Step 1: Executive Sponsorship**

- It is imperative that BCP efforts are engaged from the top. If Leadership is not interested no one else will be either...

# *BCP Planning Steps*

---



## **Step 2: Understand the Threat & Risk Environment**

- Conduct risk/threat analysis examining data available from DHS, SEMA, and local police.
- Examine infrastructure and operational implications.



# *BCP Planning Steps*

---



## **Step 3: Perform Business Impact Analysis**

- Define Planning Assumptions
- Identify business functions/processes
- Determine Recovery Time Objectives for key processes
- Identify key process interdependencies
- Examine potential financial impacts
- Identify critical resources (personnel, data, vital records, equipment)
- Identify vendors and potential resource impacts

# *BCP Planning Steps*

---



## **Step 3: Perform Business Impact Analysis...Cont'**

- Coordinate with support functions (IRM, Admin) to coordinate recovery efforts and determine limitations
- Determine Minimum Personnel Requirements
- Determine Minimum Operational Resource Requirements
- Work with IT to Determine Minimum Technology and Bandwidth Requirements
- Determine Maximum Physical Infrastructure Requirements
- Build-in executives and process owners to the future development of recovery plans

# *BCP Planning Steps*

---



## **Step 4: Develop Overarching Business Continuity Strategies**

- Form Emergency Management Team – Leadership Team to Declare Disaster and perform Command and Control.
- Form Emergency Response Team - Facility and Technology Assessment team to advise the EMT and to facilitate timely and effective decision process on plan activation.
- Develop Escalation Procedures – Describing steps that should be performed prior to and immediately after plan activation.

# *BCP Planning Steps*

---



## Step 4: Develop Overarching Business Continuity Strategies...continued

- Escalation Procedures
- Command and Control Protocol
- Corporate Communication Strategy
- Key Executive Lines of Succession and Delegations of Authority
- Resumption Strategies, including addressing transportation issues
- Training and Testing Requirements and Maintenance Plan
- **Telework Must be part of your strategy!**

# *BCP Planning Steps*

---



## **Step 5: Validate Emergency Management Plans**

- Examine emergency response plans (evacuation, etc.)
- Validate emergency communications protocol (internal and external)
- Develop/evaluate/update disaster recovery plans

# *BCP Planning Steps*

---



## **Step 6: Develop Business Unit Strategies**

- Determine practical alternatives (modes of operation) and conduct business case analysis (hot site, cold site, telework, etc.)
- Coordinate with support functions (IRM, Admin)
- Coordinate with interdependent entities (internal/external)
- Identify internal/external stakeholders of each process
- Develop emergency response plans (evacuation, etc.)
- Work with process owners to develop BC strategies
- Identify emergency operations personnel

# *BCP Planning Steps*

---



## **Step 7: Train Personnel**

- Briefings and orientation exercises
- Classroom-based training
- Online and computer-based training
- Test-based training



## **Step 8: Test Plans**

Conduct periodic tests of plans (at least annually)

- Tabletop tests
- Drills
- Functional exercises
- Simulations



### **Step 9: Develop Maintenance Strategy**

- Define roles and responsibilities
- Perform periodic updates (monthly, quarterly, annually)
- Consider structural, environment, and personnel changes
- Update strategies and personnel contact information

# *BCP Planning Steps*

---



## **Step 10: Build Employee Awareness**

- E-mail notices
- Giveaway items
- Brown bag lunches
- Organization-wide briefings
- Plan testing

# Ten Steps to Start Teleworking

---



1. Keep employees informed of the risk environment, train them on proper emergency response procedures, and direct them to health and safety responses recommended by the Federal Government

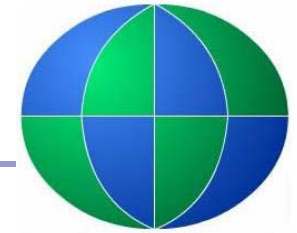
<http://www.flu.gov/professional/business/smallbiz.html>

<http://www.cdc.gov/h1n1flu/business/guidance/>

2. Craft and/or enforce policy that allows critical personnel to work remotely.
3. Use Virtual Private Network (VPN) to facilitate secure remote access.
4. Train approved personnel on the use of remote access tools and implement the immediate, though staggered, use of your teleworking tools and techniques.

## *Ten Steps to Start Teleworking*

---



6. Increase and/or test bandwidth to ensure that all critical personnel are able to VPN-in simultaneously and work effectively.
7. Virtualize critical vital records and web-enable them.
8. Consider web-based-applications for document management, enterprise resource management, and timekeeping.
9. Consider the use cloud platforms as a long term solution to make critical web applications available and accessible remotely.
10. Include telework capability in business continuity plans and implement as appropriate.

**Place the health and security of your personnel first!**

# *Questions?*

---



Please email me directly at  
[gboisson@bdaglobal.com](mailto:gboisson@bdaglobal.com)  
with any follow-on questions or comments

[www.bdaglobal.com](http://www.bdaglobal.com)

**March 31, 2010**