PRECELSUS CONSULTING

Let No One Take Away What Maria Left Us - Lessons Learned From Surviving a Cat 4 Hurricane

December 8, 2017

Larry L. Llirán, CISA, CISM

Managing Director

Precelsus Consulting

Agenda

- Introduction
- Business Continuity Standards
- Lessons Learned
- Conclusions
- Questions

1

Introduction

What do you think when you hear the name

Maria?


YAMAHA
FL6248MA

Hurricane Maria facts:

- Hurricane Maria pummeled Puerto Rico on Sept. 20 as a Category 4 storm.
- It began as a Category 5 with 175-mph winds, but it barreled through Puerto Rico as a Category 4 storm with winds up to 155 mph

- Maria is the strongest hurricane to hit Puerto Rico in more than 80 years.
- The third-strongest storm to make landfall in the U.S.
- Most of the island is still without power (79 days)
- Estimated $45 billion to $95 billion in damages to the power grid and other infrastructure.

- We have a lot to learn from this disaster.

2

Business Continuity Standards

Business continuity standards:

- British Standards Institute: BS 25999, Parts 1 and 2
- National Fire Protection Association: NFPA 1600:2010
- ASIS International: ASIS SPC.1-2009
- Australia/New Zealand Standard AS/NZS 5050
- Singapore Standard SS540
- Canadian Standard: CSA Z1600

- Government of Japan BCP Guideline
- Japanese Corporate Code – BCP
- ISO 24762 (IT Disaster Recovery)
- National Association of Stock Dealers: NASD 3510/3520
- National Institute of Standards and Technology: NIST SP 800-34
- New York Stock Exchange: NYSE Rule 4370

DRI's Professional Practices for Business Continuity Management Objectives:

1. Program Initiation and Management

- Establish the need for a business continuity program.
- Obtain support and funding for the business continuity program.
- Build the organizational framework to support the business continuity program.
- Introduce key concepts, such as program management, risk awareness, identification of critical functions/processes, recovery strategies, training and awareness, and exercising/testing.

2. Risk Assessment

- Identify risks that can adversely affect an entity's resources or image.
- Assess risks to determine the potential impacts to the entity, enabling the entity to determine the most effective use of resources to reduce these potential impacts.

3. Business Impact Analysis

- Identify and prioritize the entity's functions and processes in order to ascertain which ones will have the greatest impact should they not be available.
- Assess the resources required to support the business impact analysis process.
- Analyze the findings to ascertain any gaps between the entity's requirements and its ability to deliver those requirements.

4. Business Continuity Strategies

- Select cost-effective strategies to reduce deficiencies as identified during the risk assessment and business impact analysis processes.

5. Incident Response

- Develop and assist with the implementation of an incident management system that defines organizational roles, lines of authority and succession of authority.
- Define requirements to develop and implement the entity's incident response plan.
- Ensure that incident response is coordinated with outside organizations in a timely and effective manner when appropriate.

6. Plan Development and Implementation

- Document plans to be used during an incident that will enable the entity to continue to function.

7. Awareness and Training Programs

- Establish and maintain training and awareness programs that result in personnel being able to respond to incidents in a calm and efficient manner.

8. Business Continuity Plan Exercise, Assessment, and Maintenance

- Establish an exercise, assessment and maintenance program to maintain a state of readiness.

9. Crisis Communications

- Provide a framework for developing a crisis communications plan.
- Ensure that the crisis communications plan will provide for timely, effective communication with internal and external parties.

10. Coordination with External Agencies

- Establish policies and procedures to coordinate incident response activities with public entities.

3

Lessons Learned From Maria

Lesson #1

Backup systems

- Most organizations in PR experienced severe problems with their backup systems specially power generators and telecommunications.
- In the middle of the chaos, some organizations were forced to find a new office or even relocate their data center, while other were unable to resume operations.
- Most of the organizations were prepared for a short term electric outage, however almost none of them were not prepared to handle a long term outage.
- Were prepared for a three day outage, rather than 78 days or more, hence, they needed more equipment, data backup, power, and basically, more of everything.

Lesson #1

Backup systems

- During the first weeks after hurricane Maria struck the island, fuel suppliers were unable to get to their clients due to road blocks, the drivers did not report to work and fuel was restricted/prioritized for hospitals and critical infrastructure, among other reasons.
- The problem was even worse for organizations that relied on the renter's diligence and their contingency plans.
- Telecommunications were severely affected even when the organizations had more than one service provider.
- Many organizations rely on multiple telecommunications providers only to discover that all of the lines travel through any of several now well-known single points of failure.

Lesson #1

- Does the organization have a plan for long term electric outage?
  - Is/are the power generator(s) periodically tested?
  - Is/are the power generator(s) periodically maintained?
  - Has the landlord or administrator identified more than one company to maintain or repair the generator(s)?
  - Are there reliable suppliers /well established companies?
  - Do they have enough fuel stored to operate on power generators for a prolonged period of time?

- Has the organization evaluated their telecommunication backup strategy?
  - Has the organization evaluated its single points of failure?
  - Has identified alternate communication channels (e.g., satellite commination)?

Lesson #1

- Does the organization have a plan for a log term period without running water?
  - Do they have water storage tank(s)?
  - Is/are the water storage tank(s) periodically inspected?

- In case of leased facilities
  - Does the contract include landlord's responsibilities in case of disaster?

Lesson #2

Employees

- Many organizations experienced delays in restoring operations due to their employees were not reporting to work.
- Employees were unable to return to their work due to many factors including lack of gasoline, roads blocks, kids out of school, lack of communication with their employers, damages to their homes, etc.
- Supplies of first necessity were scarce for a certain time (gasoline, ice, food, water, batteries, etc.).
- Some continuity plans called for people to work from home, but in the event they couldn't because of the lack of power and communications.
- Institutions generally had not considered the possibility that transportation of personnel could be significantly disrupted and preclude the relocation of staff to alternate sites.

Lesson #2

Employees

- Business continuity planning had not fully taken into account the potential for wide-area disasters and for major loss or inaccessibility of critical staff.

Lesson #2

- Does the contingency plan includes to get critical staff to their locations in advance?
- Has the organization established an employee assistance program?
  - Food
  - Water
  - Shelter
  - Emergency supplies (batteries, flashlights, radios, etc.)
  - Power Generators
  - Fuel
  - Laundry
  - Daycare
  - Cash
  - Transport to an alternate location
  - Many others

Lesson #3

Suppliers / Critical Vendors

- Some organizations were unable to resume their operations as some of their critical suppliers were not operating.
- The suppliers were having trouble resuming their operations due to the same problems everybody was experiencing including road blocks, lack of employees reporting to work, lack of electrical power, lack of fuel, many others.

Lesson #3

- Has the organization established a suppliers assistance program?
  - Have identified the critical vendors?
  - Have their contacts updated and available?
  - Has established a process to timely identify critical suppliers condition?
  - Has the organization contemplated they could have to assist some of the vendors to recover their operations?
  - Have identified alternate suppliers in case one or more of them are unable to recover in a reasonable time or go out of business?

Lesson #4

Disaster recovery strategy

- Some firms arranged for their primary data center and backup facilities to be in the island.
- Contingency planning at many institutions focused on problems with a single building or system.
- Very few organizations plan for an emergency disrupting the country or region.
- Some firms lost access to both their primary and backup facilities severely disrupting their operations.
- Organizations with cloud strategies (AWS, Azure, etc.) demonstrated to be more resilient in case of a island wide disaster.

Lesson #4

- In case of a major disaster on how your main data center and disaster recovery site could get affected?
  - In-house strategy?
  - Cloud strategy?
  - Location of your main data center?
  - Location of your disaster recovery site?
  - The contingency plan scenarios include disaster disrupting the country or region?
  - The recovery strategy includes presence in the recovery site of all the production communications connections, interfaces, etc.?

Lesson #5

Communication Plan

- Communication systems is the backbone of any notification or alert system yet was one of the first things to break down during the hurricane.
- Staff were not able to access fixed line or mobile phone systems.
- The larger the company, the bigger was the problem and the harder it was to communicate with every employee, particularly employees located in rural areas.
- Local television, Internet and cable providers were heavily affected.
- Internet access was very limited.
- The more reliable communication channel turned to be the radio.

Lesson #5

- Has the organization developed a communication plan taking into consideration the main communication channels get affected?
  - What if the cellular infrastructure gets affected?
  - What if landlines get affected?
  - Is it flexible enough to address a variety of emergency situations?
  - Does the communication plan detail how communication can be carried out in the event of mass communication outages?
  - Does the communication plan contemplate the use of non-traditional communication channels such as social media to get messages to staff?
  - Does the plan contemplate to provide key staff with other communication channels such as satellite phones in case of mass communication outages?

Lesson #6

Integrated Disaster Recovery Test

- Some organizations thought they could live without some applications or services in case of a disaster, but it turned out that they really couldn't.
- Contingency planning at many institutions focus on problems with a single system.
- Plans demonstrated to only be a compliance matter and not actionable plans that will ensure continuity of services.
- There were organizations that executed a totally different disaster recovery strategy from what they had originally planned and tested.

Lesson #6

- Has the organization performed a comprehensive integrated recovery test?
  - Does the recovery tests include a scenario were the whole data center was affected?
  - Were at least all the critical applications tested in a single test?
  - Tests include interfaces?
  - Tests include third party providers?

4 Conclusions

Conclusions

- We are called to use the lessons learned from Maria in our favor.
- We need to get our business continuity strategies and disaster recovery plans to a whole new level.
- When planning, we need to assume that everything will get affected and the outage will be prolonged.
- The human factor, employees well being, is vital to resume business operations.
- It is demonstrated that compliance driven business continuity and disaster recovery plans will not be effective in a real emergency.

Questions?

References

- drii.org
- Professional Practices for Business Continuity Practitioners
- Crisis Communications Lessons Learned, DRI Canada collegiate conference Centennial college, Toronto ON
- www.sec.gov/divisions/marketreg/lessonslearned.htm

About Precelsus Consulting

We are experienced professionals that leverage proven approaches, practical experiences, and tactical problem solving skills to help our clients identify and implement the right solution to address their operational challenges.

We offer diverse consulting services that add value to the organization by helping them achieve their goals.

We have considerable experience of business, Information Technology, Risk Management, Compliance and Operations in diverse industries including banking, health and insurance. From Internal Audit co-sourcing, to requirements gathering, to project management, we provide a full range of consulting services and support to help eliminate the hassles of operations.

Visit us at - **www.precelsus.com**

Larry L. Llirán, CISA, CISM

Larry.lliran@precelsus.com

787-509-6897

