BUSINESS CONTINUITY PLAN
OUTLINE

1 Unique Role of Hotels in the Community

2 Objectives

a. Protect people (guest, employees, vendors, contractors and the public at large) from danger or more danger during a disruptive event
b. Protect physical, data and brand assets from danger or more danger during an event
c. Maintain operations to the extent possible during an interruption
d. Ensure that normal operations can be restored following the event
e. Ensure the ability to learn from the event
    i. Protect forensic data
    ii. Improve the plan

3 Definition of a Business Disruption Event

Any event that prevents the normal operations of the hotel, whether due to a local event (small fire in a hotel data center), natural

4 Response to a Disruption Event

a. Emergency Response Team – Roster, All Contact Information, Roles
    i. Internal
    ii. Corporate
    iii. External
        1. Local Authorities
            a. Police, Fire, Ambulance
            b. Secret Service, FBI, DHS
        2. Key Vendors
            a. IT Vendors
            b. Fuel
            c. Food
b. Communications During an Event
    i. Internal
        1. Radios
        2. Guest Room Annunciators
    ii. External
        1. Satellite Phone
    iii. Communications Disruptions
        1. Means for employees and families to check in with other
c. Evaluating an Event

i. Scope of Event
ii. Personal Risk Level
iii. Financial Risk Level
iv. Short-term vs. Long-term events

5 Protecting People
a. Evacuation vs. Shelter-In-Place
i. Based on Severity and Expected Duration
b. Securing the Premises
c. Guest Considerations
d. Employee Considerations
e. Supplies (“Crash Carts”)
i. Flashlight, Batteries, Glow Sticks
ii. Bottled Water
iii. First Aid Kits
iv. Battery-operated radios

6 Protecting Physical Assets
a. Securing the Premises
i. Intrusion
ii. Flood/Wind
iii. Fire Protection
b. Power Supplies
c. Water Supplies

7 Protecting Brand Assets
a. Reputational Risks
b. Communications

8 Protecting Data Assets
a. Computer Failure Contingency Plan
i. Back-up Keys
ii. Back-up Reports
b. Impact of the Cloud
i. Pro: Data stored in/backed-up up in cloud can be accessed outside the impacted area
ii. Con: If a cloud-based system is cut off due to event, no data on-site
c. Off-site Operations
d. Data Breach as an Event

9 Documentation

a. Copies of the BCP
b. Floor Plans
c. List of Entry Doors
d. Directions and Information on:
    i. Life Safety Annunciation
    ii. Surveillance System
    iii. Evacuation Plan
    iv. Computer Backups
    v. Medical & First Aid

10 Restoring Normal Operations Post-Event

11 Learning From the Event

12 Plan Maintenance & Testing

13 Sub-sections on Specific Risks
a. Credit Card Breach
b. Hurricane
c. Tornado
d. Earthquake

Disaster Recovery & Business Continuity Planning Boot Camp Case Study

HFTP Hotel

The HFTP hotel is a 4 star, city center property located in a major gateway city on the US East Coast. The 600 room property is situated along the city's Atlantic coast line offering guests great ocean views. The property is flagged under a multi-national brand and managed under a third-party management contract with a west coast firm.

The property has a full complement hotel amenities including two restaurants, in-room dining, a gift shop, and a health club with fitness and spas services as well as an indoor pool. There is 120,000 square feet of meeting and event space including a indoor/outdoor rooftop ballroom looking out over the city and the coast. The hotel also boasts a parking facility with 1200 parking spaces located below the hotel.

The hotel employs approximately 500 full-time and part-time staff, most of whom live within about 30 minutes of the property. The vast majority of staff members rely on public transportation to get them to and from work.

HFTP Hotel has another local sister property near the city's convention center. The hotel is close to public transportation with access to the commuter rail, subway and bus systems only a 5 minute walk away.

For these case studies, each group with analyze their given scenario and how it would play out if they were planning to protect the HITEC Hotel from a disruption. The disruptive scenarios are:

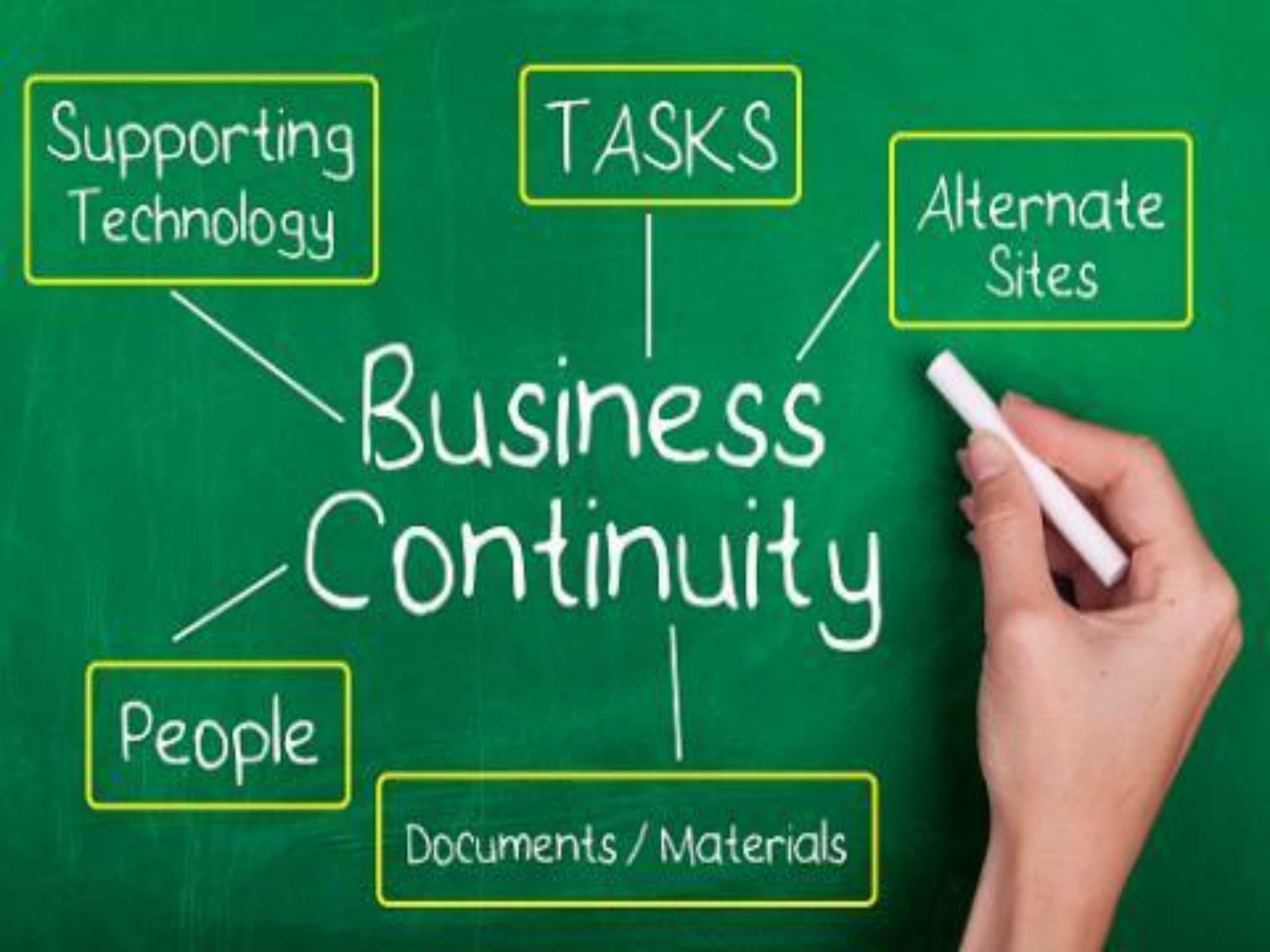
Group 1: The HITEC Hotel and surrounding businesses are crippled by a neighborhood wide power outage that appears will take 2-3 days to repair.

Group 2: Weather reports indicate that the HITEC Hotel is situated directly in the path of the season's first Category 5 hurricane.

Group 3: Multiple calls have started to come into the hotel from guests who are saying that their credit card number seems to have been compromised.

BCP – ADDITIONAL RESOURCES

Ready.gov	DHS website https://www.ready.gov/sites/default/files/documents/files/BusinessContinuityPlan.pdf
Aimnet.org	Associated Industries of Massachusetts www.aimnet.org/userfiles/files/BCP%20**Template**%202012(1).docx
MIT.edu	Massachusetts Institute of Technology http://web.mit.edu/security/www/pubplan.htm
DisasterRecovery.org	Commercial “BCP In The Cloud” service http://www.disasterrecovery.org/index.html
HFTP	HFTP guidebook on defending attacks on hotels http://www.hftp.org/i/downloads/Hospitality%20Attacks%206_16.pdf
Cornell SHA	Study on Emergency Preparedness http://scholarship.sha.cornell.edu/cgi/viewcontent.cgi?article=1006&context=chrtools


Supporting Technology
TASKS
Alternate Sites
Business Continuity
People
Documents / Materials

HITEC 2016
SM
ALL ACCESS IT
A service of HFTP
June 20–23 • Ernest N. Morial Convention Center • New Orleans, La. USA

Business Continuity Planning Bootcamp

HITEC 2016
June 20, New Orleans, LA

- Format & Agenda
  - – Overview of Business Continuity Planning (BCP)
  - – Recap of Actual Disruptive Events
  - – Small Group Breakouts Expanding Plan Outline
  - – Share Findings to Group

- What Is Business Continuity Planning?
- Why Do It?
- Unique Role of Hotels

- Business Disruption Defined

- Objectives of BCP
  - People
  - Assets
  - Operate
  - Restore Normal Operations
  - Learn

- Response to a Disruption
  - Emergency Response Team
  - Communications
  - Evaluation

- Protecting People

- Protecting Physical Assets
  - – Intrusion
  - – Flood/Wind
  - – Power Supplies
  - – Water Supplies

- Protecting Data Assets
  - – Computer Failure Contingency Plan
  - – Impact of the Cloud
  - – Off-site Operations
  - – Data Breach as an Event

- Protecting Brand Assets
  - Reputational Risks
  - Communications

- Documentation
  - The BCP Itself
  - Floor Plans
  - List of All Entry Doors

- Information on:
  - Life Safety Annunciation
  - Surveillance System
  - Evacuation Plan
  - Computer Backups
  - Medical & First Aid Resources
  - ?

- Restoring Normal Operations
- Learning from the Event

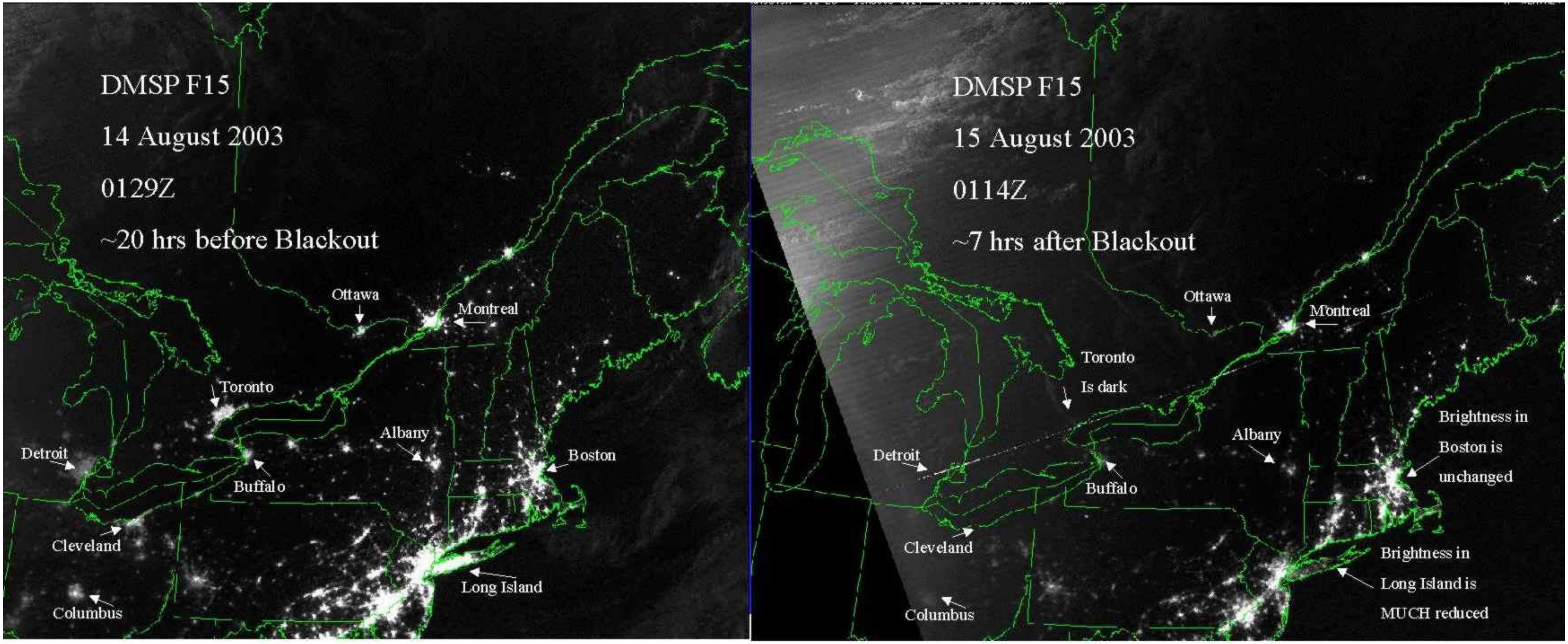
- Plan Maintenance & Testing

- Case Studies
  - NYC Power Outage 2003
  - Hurricane Katrina
  - Credit Card Breach
  - Terrorist Attack

North East Power Outage

August 14-15, 2003

- Facts About the 2003 Northeast Blackout
  - Started at approx 12:15pm in the Ohio area at First Energy due to a software glitch in an alarm system that alerts employees to possible load issues.
  - By 4:15pm, a chain reactions of outages left approx 55 million people without power in 8 different states as well as much of Ontario.
  - 508 generating units and 265 power plants were effected, mostly by “protective controls”.
  - Demand played a factor as temperatures in the impacted areas averaged 88°F.
  - Power was restored to most areas within two – three days. Prompt recovery was credited in part to technology put in place in preparation for Y2K.
  - 12 deaths were attributed to the blackout
  - US DOE estimates the financial impact of the blackout was $6bn



DMSP F15
14 August 2003
0129Z
~20 hrs before Blackout

DMSP F15
15 August 2003
0114Z
~7 hrs after Blackout

- Four Seasons New York Experience – Positives (thanks to good planning/design)
  - Great emergency power (generator & UPSs)
  - In-building communication: radios/pagers, PBX, LAN
  - Redundant cooling for data center
  - Voice & data circuits available for first 8-10 hours
  - Cell phone service worked on street
  - Plenty of water bottles stored for emergencies
  - Bulk of building refrigeration on emergency power
  - Low enough occupancy that staff could stay in rooms
  - One day only outage allowed us to get by with limited supply deliveries

- Four Seasons New York Experience - Opportunities
  - Validate that all necessary equipment is supported by emergency power
    - Pumps for fresh water supply
    - Exhaust hoods
  - Tank-less toilets proved to be an issue, could not manually fill
  - Limited AC due to lack of functioning cooling tower
  - TV service was down. Guests could not understand true impact of outage at other properties
  - Emergency communication to the outside required review, possible satellite phone as future backup
  - Better communication as a team regarding response and planning.
  - Additional redundancy for voice & data circuits routed through alternate “last miles”
  - May have struggled with a diesel fuel delivery

gettyimages
Matthew Peyton
2401399

gettyimages
Matthew Peyton
2401403

<u>Northeast Blackout Post-Mortem Study</u>:

“Safeguarding Service: Emergency Preparedness Essentials” by Robert J Kwortnik, Ph.D. Cornell University

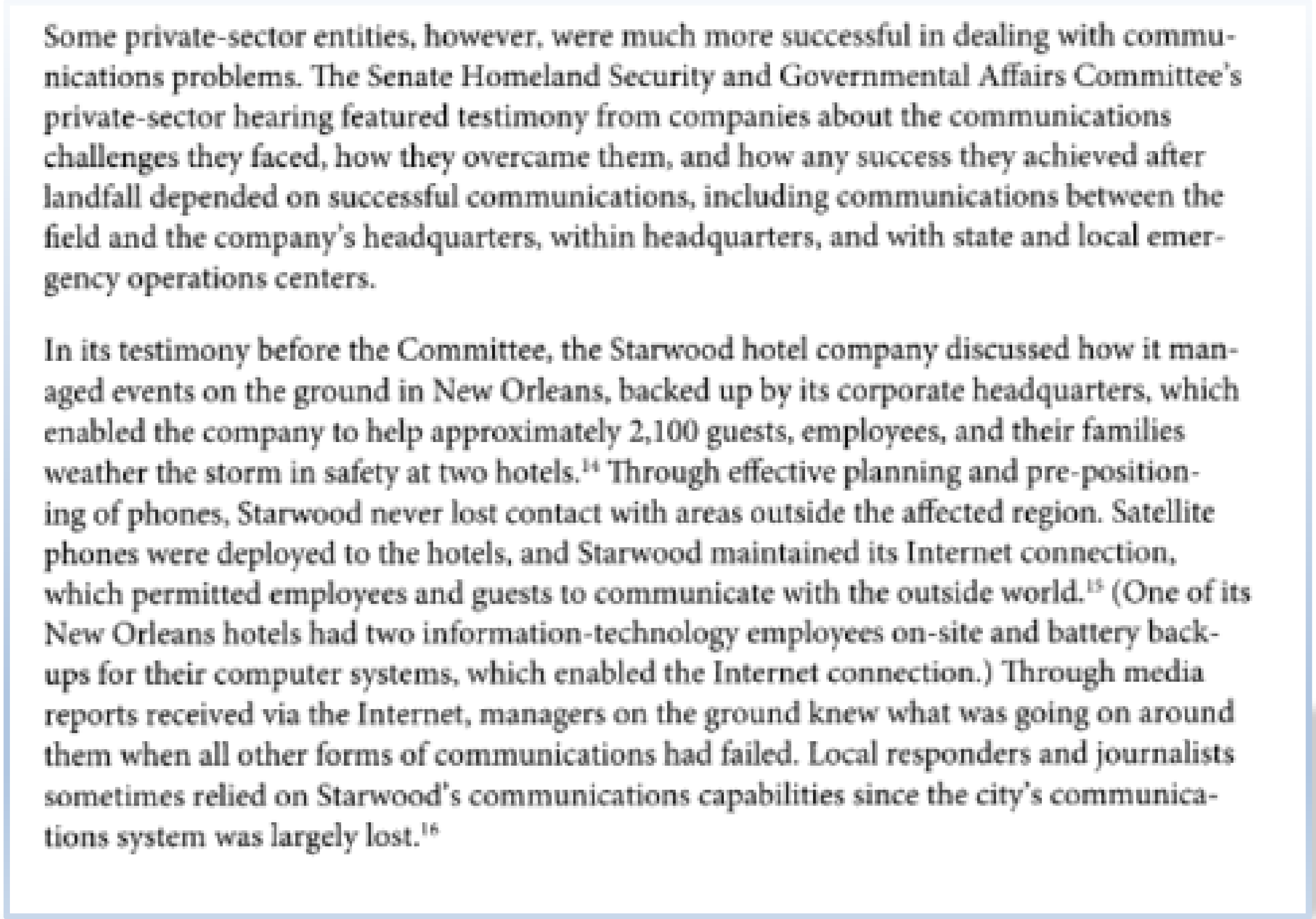
http://scholarship.sha.cornell.edu/cgi/viewcontent.cgi?article=1006&context=chrtools

Hurricane Katrina

August 23-31, 2005

- Facts About Hurricane Katrina
  - Hurricane Katrina was the largest and 3rd strongest hurricane ever recorded to make landfall in the US
  - In New Orleans, the levees were designed for Category 3, but Katrina peaked at a Category 5 hurricane, with winds up to 175 mph
  - The storm surge from Katrina was 20-ft (six meters) high
  - An estimated 80% of New Orleans was under water, up to 20 ft deep in places
  - The final death toll was at 1,836, primarily from Louisiana (1,577) and Mississippi (238)
  - Hurricane Katrina caused $81 billion in property damages, but it is estimated that the total economic impact in Louisiana and Mississippi may exceed $150 billion, earning the title of costliest hurricane ever in US history

- Sheraton New Orleans Katrina Tactics
  - Before the Storm reviewed the Business Continuity Plan:
    - Executive Chef placed orders for food, supplies and bottled water
    - Diesel Tanks are full and functioning
    - Ensured all essential areas are powered by the emergency generator
    - Secure the checklist items “flashlights, batteries , glow sticks and batteries operated TV’s and Radio’s”.
  - During the Storm
    - Hotel Guests gathered in the Grand Ball Room (700+ Guests)
    - Warm food & Water was plentiful.
    - Hotel IT team was able to provide kids movies for entertainment plus Free internet & Long Distance dialing to all guests
  - After the Storm
    - Management arranged for evacuation for the Guests and the Employees and their families
    - Relocating employees to Houston, Dallas and Atlanta.
    - Within 10 days, establishing a remote Sales Office at the Westin Peachtree Plaza with all required data “PMS – Sales – Public & personal Folders”.



Some private-sector entities, however, were much more successful in dealing with communications problems. The Senate Homeland Security and Governmental Affairs Committee's private-sector hearing featured testimony from companies about the communications challenges they faced, how they overcame them, and how any success they achieved after landfall depended on successful communications, including communications between the field and the company's headquarters, within headquarters, and with state and local emergency operations centers.

In its testimony before the Committee, the Starwood hotel company discussed how it managed events on the ground in New Orleans, backed up by its corporate headquarters, which enabled the company to help approximately 2,100 guests, employees, and their families weather the storm in safety at two hotels.[14] Through effective planning and pre-positioning of phones, Starwood never lost contact with areas outside the affected region. Satellite phones were deployed to the hotels, and Starwood maintained its Internet connection, which permitted employees and guests to communicate with the outside world.[15] (One of its New Orleans hotels had two information-technology employees on-site and battery backups for their computer systems, which enabled the Internet connection.) Through media reports received via the Internet, managers on the ground knew what was going on around them when all other forms of communications had failed. Local responders and journalists sometimes relied on Starwood's communications capabilities since the city's communications system was largely lost.[16]

Credit Card Breach

Business Continuity and Resiliency

Business Impact Analysis

Define what we are protecting and who is responsible for protecting it

It is critical that organizations develop, implement and test their business continuity plans. Historically Brands have a higher level of maturity due to availability of resources but their plan seldom addresses the managed or franchised location.

Today's landscape requires franchisees and management companies to have a well thought out, all inclusive BCP that takes into account not only the physical but cyber perils.

Business Continuity

Historically BCP’s fail to include Security in plan development and testing. Security is viewed to be Accountable or Informational instead of Responsible (RACI). When cyber-disruptions occur we rarely see BCP’s engaged and this causes confusion and a disjointed handling of events.

Incident Response must be part of Business Continuity Planning

Continuity and Hospitality

SaaS solutions – if we lose internet access for an extended period of time we lose connectivity to our Property Management System the Point of Sale, Guest Internet and possibly voice communications.

In the case of a suspected breach a determination needs to be made as to shut down outbound access, or take key systems offline for extended periods.

In a case where authorities walk into a merchant demanding the PMS or POS in order to take it for imaging (case study) we need to have a BCP in place to address the impact to the business

BCP in Hospitality is not a one size fits all model.

Lets consider the following operating models

Brand owned property

- Robust Infrastructure
- Perhaps multiple points of Internet Access
- Covered under the brands continuity and contingency planning

Brand Managed Property

- Infrastructure
- Reliance on Brand resources for continuity

Third Party Managed Property

- Infrastructure varies from property to property
- Lack of a formal network or security support model
- Management Company may provide core services but there is rarely a BCP that covers issues at the property level
- There is no Incident response plan
- REACTIVE which extends the outage period and impact to the merchant.

Individually Owned and Operated

- Very immature in terms of infrastructure, controls, or planning
- Support model is limited or non-existent in many cases
- There is rarely a contingency plan in place and all actions (right or wrong) are ad-hoc in nature.
- Panic sets in
- Out of business

Business Continuity in the Face of a Cyber Attack

Business continuity plans provide guidance and order in the face of chaos

CASE STUDY – Based on a real life Incident

- We are working with a mid-sized 250-350 room count property located in the center of a major city.
- There are three primary types of guests. During the week the property is host to business travelers who normally check in on Sunday and check out on Thursdays, Tourists and Sports enthusiasts who come to see live sporting events.
- Given the properties proximity to a major sports venue the property is typically sold out on the weekends hosting guests from all over the country.
- A large portion of the properties revenue comes from food and beverage outlet located on property.
- This weekend is the final playoff game and the property expects to be sold out and have one of it’s largest revenue weekends all year.

Ownership

The property is owned by a Major REIT and is managed by a company located across the country. The management company provides limited security services and uses a third party entity for break fix support.

Technical

The property uses a premise based property management system and a SaaS Point of sales solution. There is a domain with about 50 desktops and servers on a large flat network.

On Wednesday at 1:49am the night auditor receives a call from local authorities. They tell the auditor that they believe the property is subject of an active and ongoing cyber-attack and that credit card data is being actively exfiltrated to a third party entity.

The U.S. Secret Service Agent wants to come in and take custody of the Property Management System so it can be imaged for forensic testing purposes.

They will have the server for approximately 3 days. They also recommend shutting down Internet access until the firewall rules can be reviewed and an “unofficial” forensic audit can take place to determine IF and WHERE the loss of data is coming from.

Shutting down external access will prohibit the SaaS Point of Sales System from working because it does not support offline transactions.

The night auditor attempts to contact someone at the management company but it is late and no one answers.   He contacts the third party help desk support line who escalates to tier 2 and is told just shut off the box (he doesn't have the context that the "box" is the PMS and can't be just "powered down" and the cardinal rule of forensics is you don't power down a potentially compromised system.

Authorities are coming in at 7:30 on Thursday to take custody of the server which means there will be no check-outs.

<u>What does the Property Do to get past this challenge and prevent future similar events?</u>

ASSUMPTIONS

1) When the FBI or U.S. Secret Service are involved there is a high level of certainty that a data breach is or has occurred.

2) We have contacted the Brand and their stance is that since this is an independently owned and operated property with their own security infrastructure in place and unique PMS / POS configurations they will not be able to offer much in the way of technical support.

TERRORISM

- Disruptions Due to Terrorism
  - Various scenarios including active shooters, bombings, hostage taking, chemical or biological attacks, etc.
  - Great resource on this topic is the HFTP article written by Eliza Selig and Frank Wolfe titled “Hospitality Attacks: Tips That Could Save Lives

- No location is safe. As noted by Stratfor Global Intelligence, hotels are “soft targets”
- Need to think about things such as:
  - Local law enforcement’s training and willingness to assist, varies by location
  - Realistic threat assessments by experts including focus on equipment and physical security measures
  - Training and drilling of all staff, not just security. Being alert for signs of suspicious activity
  - Physical backup of data to be used during emergency. This includes hotel systems as well as building drawings
  - Communication plans and use of social media
  - Location of key security facilities and access to those facilities in an emergency

HITEC℠ 2016

ALL ACCESS IT

A service of HFTP