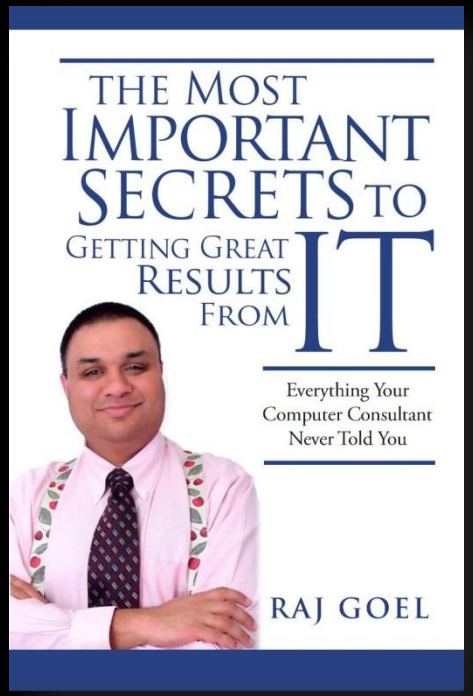
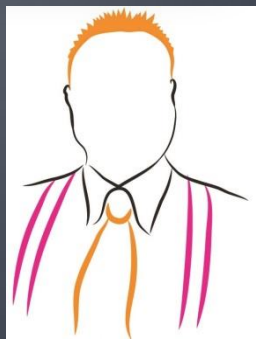
Lessons Learned From Sandy

Raj Goel, CISSP
raj@brainlink.com / 917-685-7731
www.RajGoel.com
www.ITSecurityConsultant.com
@RajGoel_NY





Handouts

Grab them from

www.RajGoel.com/surveillance-notes/



©2013 Raj Goel / Raj Goel, CISSP / raj@brainlink.com / 917-685-7731

Murphy has plans…



© Bob Gorrell, www.GorrellArt.com

…and he executes better than you.

In the last decade, New York City has experienced:

- Multi-state power blackouts
- 9/11 World Trade Center Collapse
- Con-Ed steam pipe explosions
- Tornadoes & Cyclones
- Earthquakes
- Sandy



NYC On A Normal Night



NYC - Sandy



Absolute power corrupts absolutely…





…but we still need gas.

- For the 1st time in decades, NYC implemented gas rationing.
- Even is people had power in their homes, and their neighborhoods were functioning, lack of gasoline kept people at home.



Nuclear reactors pack a lot of power…

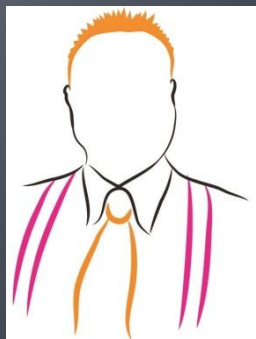


…but water is still king.

- Rising tides & storm surges caused 5 nuclear reactors to go offline.
  - (Fukushima Daiichi problems were multiplied by ocean water flooding the backup generators).
- Reactors going offline or being forced offline caused further strain on the electrical grid



Disaster Recovery & Business Continuity Lessons



1) In a flood zone, don't put transformers or generators in the basement

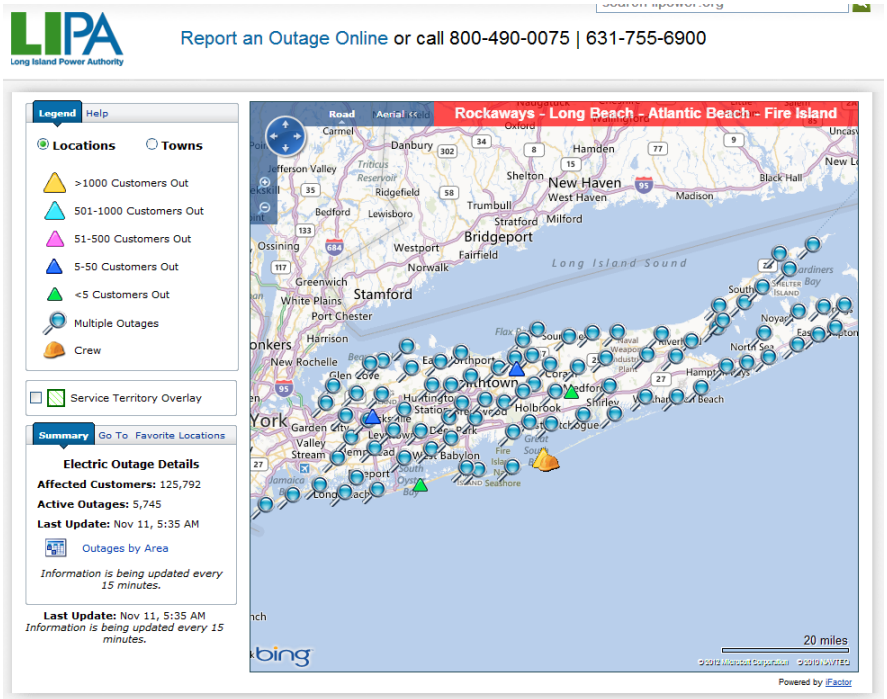


- If you live in a flood zone, putting transformers or generators in the basement isn't the smartest idea.

- Nurses and staff saved countless lives by carrying patients out of the hospital manually. NYU's BCP & DR plan was inadequate.



2) Utility outage maps are crucial



- Just like pizza, even bad ones are better than nothing.

- Even after LIPA & ConEd stopped updating their maps, knowing which areas were out, and which ones were functional allowed us to deal with employees better.



3) Redundant generators are awesome



…as long as you have redundant fuel as well.

- Peer 1's data center had generators on 2nd floor.
- Peer 1 had their own generator on 17th floor as backup.
- Basement flooded – building generators offline. Peer1 kept running…until diesel almost ran out.



4) Cash is King



- Normal Hertz rate: $300/wk
- Sandy rates: $2000/wk

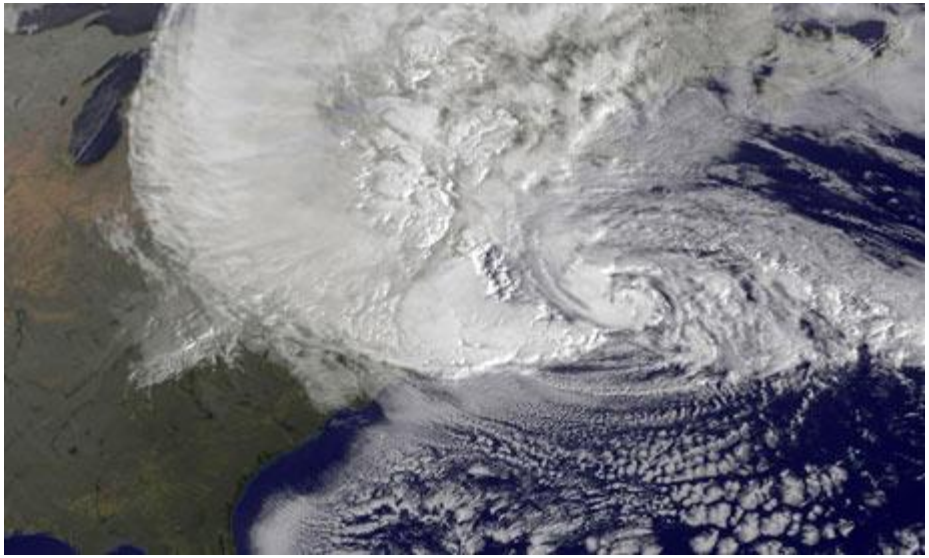
- Normal hotel rate: $300/night
- Sandy rates: $800/night

- Helicopter hired by photographer Iwan Baan required cash up front to charter the chopper.

- We had spare servers, drives, switches & firewalls set aside for clients BEFORE the storm.
  - Do you?



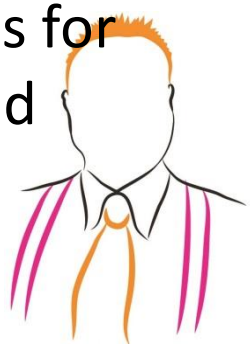
5) Geographical redundancy matters



- A large, multinational firm with thousands of employees globally hosted their exchange servers from NYC HQ. NYC lost power for a week.

- No one had emails…globally.

(CIO/COO had rejected previous recommendations for redundant data centers and offsite backups).



6) Leadership matters



1) Shutting down the traffic tunnels and subway lines was the best decision NYC's government made.

2) Keeping cars and unnecessary vehicles off the street was a smart decision. This also made subsequent recovery faster.

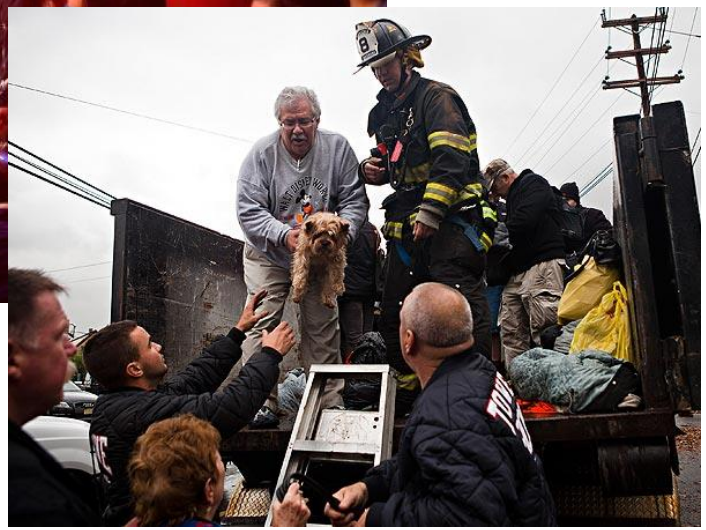
3) Chris Christie (NJ Governor) calling mayors stupid for not evacuating when ordered to – SMART!

Saved thousands of lives and billions in losses.



7) People are your BEST assets





- Are your employee contact lists up to date?
- Do you have out-of-state next-of-kin info?
- Cellphones? IM/Skype IDs? Home phones? Spouse & children names, ages, contact info?
- Prescription & OTC medications on hand?



8) Post-Event Communication

Fix&Fortify SANDY RECOVERY WORK

- NYC MTA has plastered these signs across all the train stations, tunnels, bridges that they are repairing OR strengthening

- How does your firm communicate post-disaster / post-breach cleanup and remediation?



How we dealt with Sandy

Before the storm

1. We tested all client backups in the DR center
2. Ensured we have contact info for clients, client staff, family members
3. We published the DISASTER PREPAREDNESS TIPS page
    - http://www.brainlink.com/2012/10/tropical-storm-sandy-disaster-preparedness-tips/



How we dealt with Sandy

During the storm

1. I published a daily blog updating clients (and others) with resources for recovery.
    - http://www.brainlink.com/2012/10/sandy-recovery-resources/
    - Free or low-cost office space, places to sleep or get hot food, hot showers, etc.
2. Called, texted, skype'd clients, employees, family members for 48 hours.



How we dealt with Sandy

After the storm

1. We visited every client
2. Replaced many UPSes and power strips
3. Reviewed DR & BCP Plans
4. Clients purchased redundant / backup circuits for single-homed clients
5. More clients adopted virtualization



Summary

1. Large, unprecedented events will happen more frequently
2. Review building codes and best practices
3. Power (and fuel) is KEY.
4. Budget for spare resources.
5. Geographical redundancy is imperative
6. How your city or state plans for disasters MATTERS!
7. People are more important than technology



Humor

- Patron: **“Barkeep, make me a Sandy!”**
- Barkeeper: **“What’s that?”**
- Patron: **“You know…a watered down Manhattan :-) “**

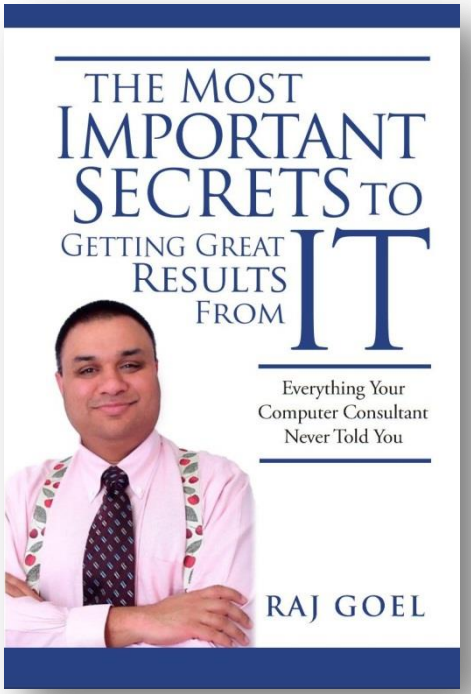
- **They should have named the storm A-Rod.**
- **Why?**
- **Because then, it wouldn’t have hit anything.**



Contact Information

Raj Goel, CISSP

C: 917-685-7731
raj@brainlink.com
www.RajGoel.com
www.linkedin.com/in/rajgoel
www.ITSecurityConsultant.com
@RajGoel_NY



Author of "The Most Important Secrets To Getting Great Results From IT"
http://www.amazon.com/gp/product/0984424814



©2013 Raj Goel / Raj Goel, CISSP / raj@brainlink.com / 917-685-7731