Disaster Recovery Planning

Diversity in the workplace isn't just for people

whois Ken Scott aka pwrcycle

- Positions with: Salesforce, F5 Networks, Apple, Verisign, Prolexic
- 11 years as a DDoS Security Engineer
- Trained dozens of SOC engineers
- Written several Incident Response & Disaster Recovery Plans

Things That Cause Disasters

Disaster = Anything that prevents many from doing work for an extended period of time. DRP addresses "Availability"

- Natural Disasters
- Construction
- Squirrels
- Hackers

(Sysadmin's mentality: all problems are squirrels until proven otherwise)
(Occam's razor: the simplest solution is usually the right solution)

Disaster Recovery Process

1. Step back.
2. Take a breath.
3. Identify the priorities. What service/process are you trying to keep up?
4. Identify the options. What service are you using that you can route around?

Diverse Locations
Diverse Systems
Diverse Methods

Something happened. What do you do now?

Disaster Recovery Plan should be part of your Incident Response Plan.

- Don't Panic
- Find a way to communicate
- Assemble a team
- Assess the situation
- Get control of the situation

Planning: The Big Red Folder on the Shelf

- Phone numbers (including personal phone numbers)
- Designate a central rally point of communication
- Internal Communication
  - Email (Exchange / Gmail / Protonmail / Twitter DMs)
  - Text Chat (Slack / Hipchat / IRC)
  - Voice Chat - (Hipchat / Google Hangout / GoToMeeting)
- Diversity of Systems (Windows / Linux / Mac)

Here we go

- Establish Internal Communication
- Limit External Communication (Yes, there is a problem & we're working on it.)
- Divide timeframes into short / medium / long term.
  - 1 Hour = Short Term
  - 4 Hours = Medium Term (1 hour to: Talk, Act, Assess, Relay)
  - 12 Hours = Long Term
- Keep groups small; 6-7 people. Don't put too many cooks in the kitchen.

- Assemble information. Turn copypasta into PR Poetry.

This ain't poetry we're writing here.

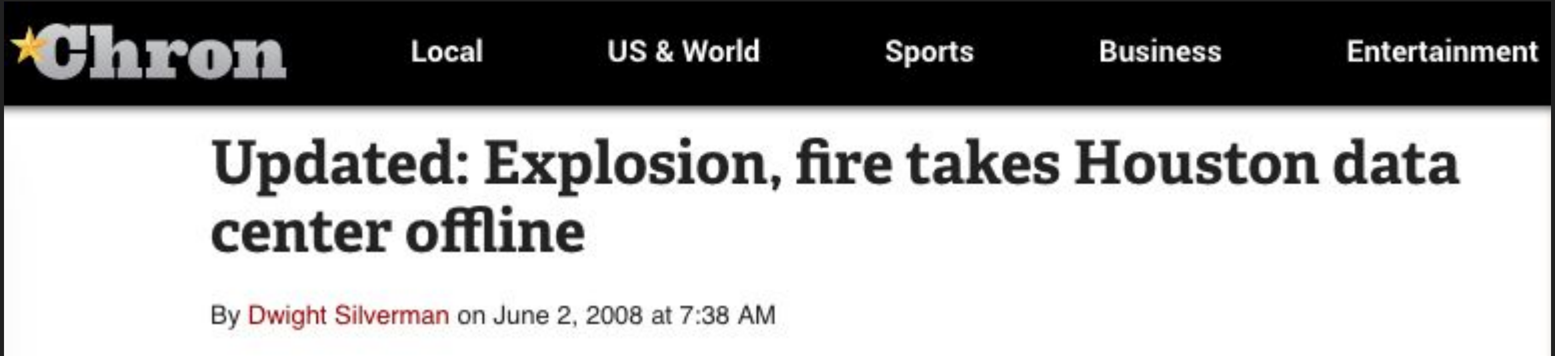
Be succinct.
Don't use adjectives.
Don't use metaphors.
Don't use hyperbole.

Don't send an email with an IP in it.
Reports? From who? From where?
Details matter most in the early stages.

The web server did not "blow up".
It was not the "Pearl Harbor" of cyber attacks.

Packets are not bullets.
Exploits are not hand grenades.
We are not at war.

The Day ThePlanet blew up



Updated: Explosion, fire takes Houston data center offline

By Dwight Silverman on June 2, 2008 at 7:38 AM

https://blog.chron.com/techblog/2008/06/updated-explosion-fire-takes-houston-data-center-offline/

"Three walls of the electrical equipment room on the first floor blew several feet from their original position, and the underground cabling that powers the first floor of H1 was destroyed."

ThePlanet explodes: Life after a Death Star

Even though he assured diversity by the provider, the end-customer did not realize these servers were all in the same data center.

- website
- support site
- DNS servers
- email servers

They had a backup site on a different provider, but no way to change to that provider. Instructions for his NameServer host were in his unreachable email. The last DNS record pointed to my service with a 24 hour TTL. He was at an airport.

I could verify the explosion via news articles.

Luckily, he had, at some point, given a secondary phone number.