Cyber Disruption Response Planning

May 13, 2015

Jonathan Wiggins, Regional Planner
City of Houston, Mayor’s Office of Public Safety and Homeland Security
Setting the Stage

- What *cyber* means to me
- We’re talking left of boom
- My questionable credentials
Why cyber disruption planning?

• Chance of attack/adverse incident
  – Cyber attack
  – Natural disaster
  – Accidental damage

• Chance of vulnerability within the system
  – Operating system/application vulnerability
  – Unavoidable vulnerabilities/physical presence
Cyber Attacks
Natural Disasters
Intentional Damage
Unintentional Damage
Pandemic Incident
Science Fiction?
Science Fiction?
Science Fiction?
Science Fiction?
But, seriously...
Consider the following...

- Power is out, possibly for weeks
- 50% of your electronic equipment is damaged
  - Cellphones
  - Computers
  - Radios
  - Networking equipment
  - Cars
  - Gas pumps
  - Sewage pumps
  - Medication dispensers
  - Traffic lights
  - Refrigerators
  - Washing machines
  - Coffee makers
Who do you turn to?

I GOT 99 PROBLEMS

BUT A GLITCH AIN'T ONE
Who do you turn to?
The Disconnect

Emergency Managers

IT Professionals
That’s where we began.

• Three workshops designed to
  – Bring EM and IT together
  – Invite law enforcement
  – Establish a framework
  – Guide plan development
Workshop 1: Executive Overview

- Engage executive management
- Establish a cyber disruption planning framework
  - Plan for large/long-duration disruption
    - Effects-based planning
    - Cyber disruption teams
  - Integrate/Share best practices among EM and IT
- Get buy-in from all
- Give them homework
Effects-based Planning

• Loss of data
• Loss of access to desktops
• Loss of power
• Loss of staff
• Loss of local equipment
• Loss of Internet
• Loss of LAN/WAN resources
• Loss of supporting infrastructure
Cyber Disruption Teams

• CDTs understand:
  – Nature of cyber disruptions
  – Effects on critical cyber assets
  – Response activities
  – Potential resource needs
    • Re-establish operations
    • Maintain
    • Protect
CDT Membership

- Composure and role determined by jurisdiction/agency
- Core members (operations)
- Associate members (supplemental)
CDT Preparedness Activities

- Identify and address threats and vulnerabilities (CDRAT)
- Communicate with other jurisdictional CDT representatives to exchange best practices and information pertinent to preparing for cyber-related incidents
CDT Response Activities

- Work within the ICS structure to provide situational awareness, subject matter expertise, and potential solutions
- Provide other CDTs with situational awareness and assistance during an incident as necessary
- Monitor incidents and share information among other CDTs
CDT Recovery Activities

• Determine resources needed to restore operations to a normal state
• Track restoration efforts and provide information regarding time to full restoration
• Conduct after-action reviews to obtain lessons learned following an incident
Workshop 1 Homework

- Tri-fold brochure
- Tasks for each discipline
  - Meet with
  - Learn about
  - Evaluate capabilities
  - Plan for
Workshop 2: Plan Development

• Purpose
  – Discuss products
  – Bring partners to the table
  – Fill out worksheets in jurisdictional groups

• Goal
  – Written record to inform planning
Worksheets

• Complemented template
  – Heavy on CDTs
  – Addressed major questions and issues
  – Activation, operations, and communication

• Written record
CDT Training Guide

- Lists free/low-cost courses:
  - EM courses for IT personnel
  - IT courses for EM and LE
  - Introduction-level, advanced-level, courses for management
- Includes a sample training plan for each role within the Cyber Disruption Team
Cyber Disruption Readiness Assessment Tool

The Internet is down and all the music is dead. The future sucks!

It's alright. It's okay. Listen. I found this ancient CD-R. Maybe I had the foresight to burn some MP3s on it.

Noice. That's Australian for...

It's just Glycerine? By Bush? You burned a whole disc for one song?

Never again.

The aughts were a heady time.

We trusted the cloud, and it's made fools of us all!
Cyber Disruption Readiness Assessment Tool

- Built on effects-based approach
- Points out areas where sufficient capabilities exist
- Provides information to help improve capabilities in less-developed areas
- Generates a checklist report of to-do items
Workshop 3: Test Plans

• Exercise plans
• Continue plan development
• More worksheets
• Jurisdictional groups
Scenario

- Fire at a datacenter run by the jurisdiction
  - Damage from heat, smoke, water
  - Unknown cause and level of damage
  - Significant resources to restore functionality
- Incident was at 6:30 p.m.
- Incident continued through next morning
Three Modules

- Module 1: CDT purpose, role, and activation
- Module 2: Role continued, communication among members, who is in charge?
- Module 3: Internal and external communication
After-Action Report

• Common strengths:
  – Role of the CDT
  – Use of established processes

• Common areas for improvement:
  – Plan activation triggers
  – Roles and responsibilities
  – Assigning authority
After-Action Report

- Additional recommendations:
  - Definition of cyber disruption
  - Cross-discipline training
  - Continued planning efforts
Current Activities

- Plans are progressing but slowly
- Right people getting onboard
- Lots of excitement from IT staff
Questions?

Jonathan Wiggins  
Regional Planner  
COH, Mayor’s Office of Public Safety and Homeland Security  
jonathan.wiggins@houstontx.gov  
832-393-0933

All resources and materials available at  
http://www.houstonuasi.com/go/doctype/1532/213293/  
(HoustonUASl.com > Resources & Plans > Cyber Disruption Planning)