NERCPI Regional Cyber Disruption Planning

NEW ENGLAND
REGIONAL CATASTROPHIC
PREPAREDNESS INITIATIVE

URS

www.newenglandrcpi.org

Cyber Disruption Planning

- Catastrophic cyber planning is an evolving concept
- True emergencies vs. inconveniences
- Fully interconnected world
  - SCADA
  - SmartGrid
  - Stuxnet
- Do we know what we don't know?

URS

NERCPI

Why does Cyber matter to EM?

URS

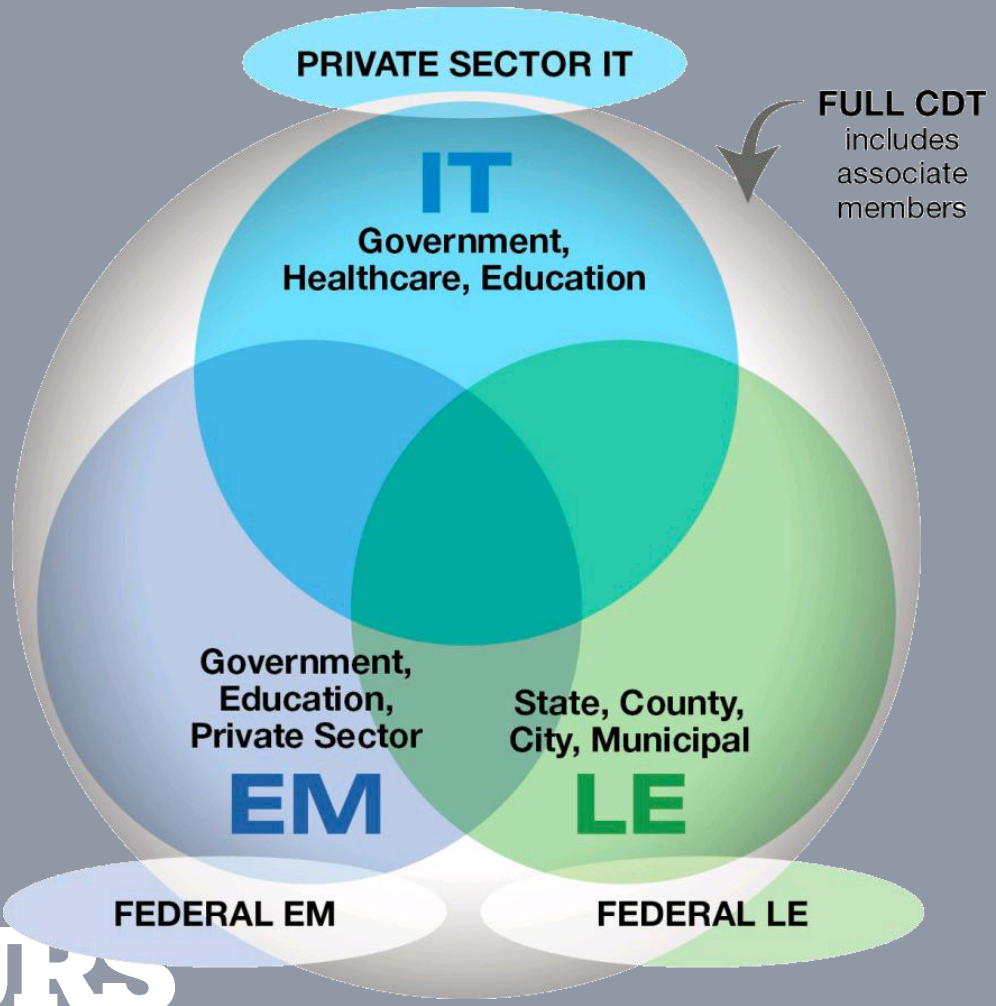
Planning Process

- Identify Assets
  - CIKR vs Cyber Assets
- Determine Capabilities of Assets and Personnel
- Analyze Risk to Assets and Region
- Current State
- Integration with other Regional Plans
- SHARING INFORMATION

URS

NERCPI

Cyber Disruption Team

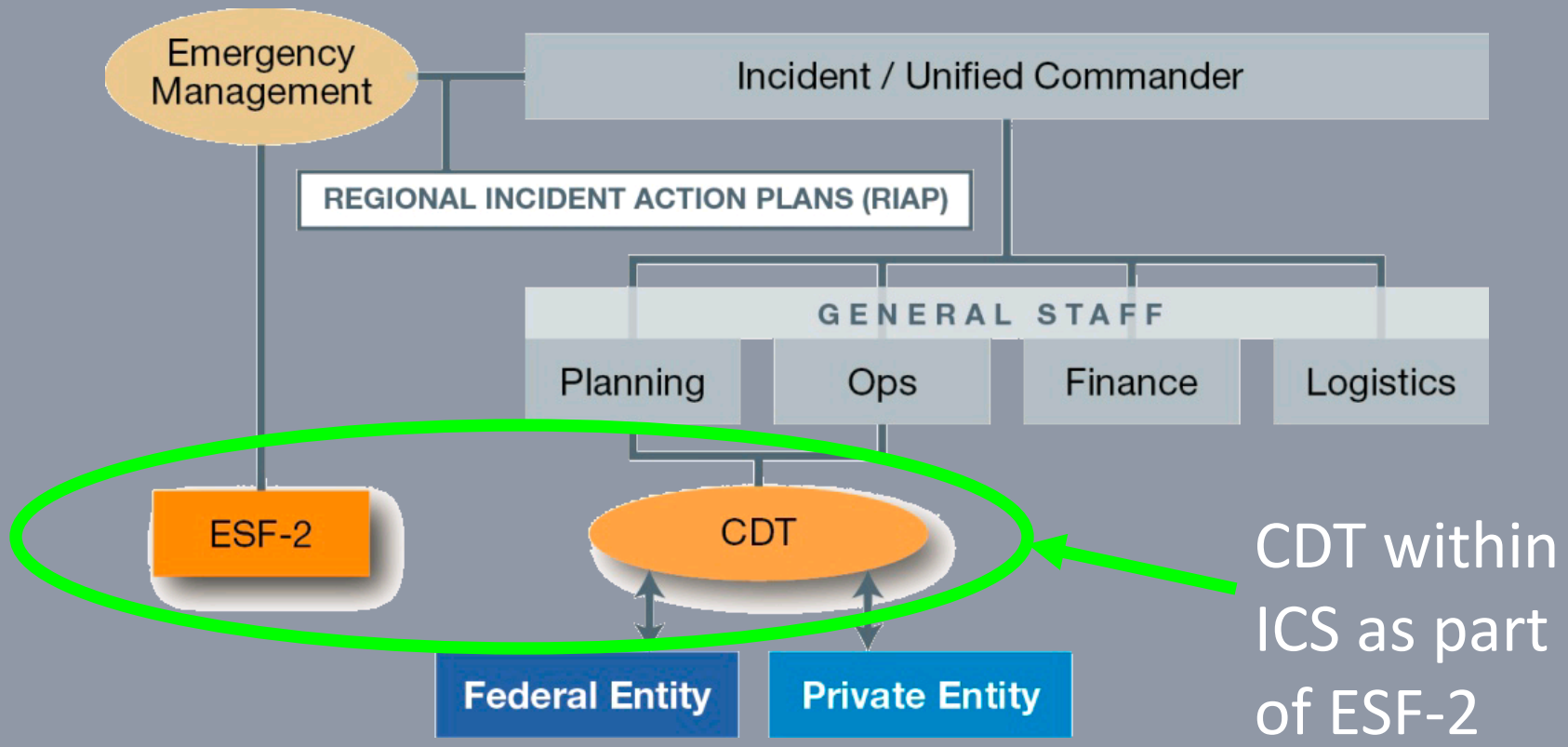


The ***CDT*** is the cadre of experts available to manage or assist the management of a critical incident.

URS

NERCPI

Cyber Disruption Team



URS

NERCPI

Regional Structure

- CDT within each jurisdiction
  - Template adapted differently in each jurisdiction
- Regional Cyber Disruption Response Annex
  - High level multi-state CDT coordination
- Training Strategy
  - Recommendations to be implemented by CDTs, based on standards
- Resiliency Annex

URS

NERCPI

Project Completion

- ‘Completion’ is a misnomer for this project
- Can look towards 1 – 3 – 5 year goals:
  - ***1 yr – Memorialize gains and lessons learned***
  - 3 yrs – CDTs have grown in membership and representation. Other agencies have formed CDTs.
  - 5 yrs – Cyber disruption response more closely mirrors other types of response (law enforcement, fire, etc.). Resources are typed.
- Centers of Excellence

URS

NERCPI

Lessons Learned

Lesson Learned #1 – What is Catastrophic

- Catastrophic = we'll know it when we see it
  - Sustained impairment of a critical business process
  - Loss of a system that protects life, health, safety
    - Hard to map 2° and 3° dependencies/impacts
  - Physical damage to critical cyber asset

URS

NERCPI

Before….

Events	Incidents	Disasters
Login	Lightning strike	Small Hurricane
Logout	Loss of PII data	Localized flooding
Port scan	Unauthorized access	Temporary power outage
Create new user	Localized virus infection	Temporary Internet outage
Attempt to connect	Localized worm infection	Localized virus infection
Application start/stop		Localized worm infection

URS

NERCPI

Events

Login
Logout
Port scan
Create new user
Attempt to connect
Application start/stop

Incidents

Lightning strike
Loss of PII data
Unauthorized access
Localized virus infection
Localized worm infection

Disasters

Small Hurricane
Localized flooding
Temporary power outage
Temporary Internet outage
Localized virus infection
Localized worm infection

Catastrophe

…After

Large Hurricane
Regional flooding
Sustained DDOS

Extensive virus / worm infection
Sustained power outage
Sustained Internet outage

Loss of all supporting Infrastructure
Physical Damage to a Critical Cyber Asset

URS

NERCPI

Threat Assessment on Critical Cyber Assets

- Traditional threat assessment was difficult because catastrophic = low probability / high impact events
  - How manage risk of ‘black swan’ events?
- Changed focus of assessment to effects-based planning
  - Many possible causes led to finite number of effects

URS

NERCPI

Ice Storm

Radiological Dispersion Device

Earthquake

Worm Infection

Solar Flare

Power plant hacked

Hurricane

Swine Flu

Denial of Service

Cable Cut

Desktop hacks

Nuclear Attack

Ice Storm
Radiological
Dispersion
Device
Earthquake
Worm Infection
Solar Flare
Power plant hacked
Hurricane
Swine Flu
Denial of Service
Desktop hacks
Cable Cut
Nuclear Attack

Scenario Effects

Loss of Power
Loss of Internet
Loss of LAN/WAN
Loss of access to desktops
Loss of local equipment
Loss of all supporting infrastructure

Lesson Learned #2 – Effect-based Planning

- Effects-based planning was very successful in getting disparate groups to come together to focus on how to make the [business/system/process] better
  - Talking about threats was adversarial
- Executive-level managers could better relate to the risk-management issues

URS

NERCPI

Reliance on IT Systems

- Conversely, Executive management was often terribly unaware of the reliance on the 'cyber' infrastructure
  - Routinely found that departments / organizations had no IT contingency plans
    - No knowledge that system had IT interconnections, or
    - Believed that the 'IT Department' would fix systems, provide desktop resources, etc.
- Specifically, Emergency management was not aware that ops would be crippled without IT

URS

NERCPI

Lesson Learned #3 – IT Dependence

- Hard to conceptualize, map, and articulate all the interdependencies related to the cyber infrastructure
  - Unknown and unintended consequences are probable.
    - "I don't know" is a very real answer
  - The effects-based planning helped mitigate risk associated with unknown interdependencies or dependencies out of your control

URS

NERCPI

Managing Large Incidents

- The Emergency Management community is really good at managing chaos
  - They plan incessantly, write everything down and have very structured response / recovery organization, management and procedures
  - Can we say the same about our COOP / IT DRP…?
- EM's job is to help those with domain expertise excel in a stressful situation

URS

NERCPI

Lesson Learned #4 – IT Learn from EM

- Catastrophic Cyber Disruptions cannot be managed with a 'helpdesk' mentality
- Nor can the IT Dept handle the disruption alone without assistance / interference
- We learned there was significant benefit to incorporate EM training and principles into an IT DRP / Disruption Response
  - Incident command system, span of control
  - Incident Action Plans, external resources

URS

NERCPI

Lesson Learned #5 – Cyber Disruption Planning Halo Benefits

- Identify Critical Cyber Assets and talk with asset owners and operators
- Create a multi-disciplinary Cyber Disruption Response Team
- Provide IT personnel with EM training
- Train EM personnel on IT systems
- Exercise response and recovery actions
- ….Are we better off regardless of whether a catastrophic even occurs?

URS

NERCPI

Questions?

URS

NERCPI

Thank you

Adam Wehrenberg
RCPGP Project Director
City of Boston OEM
617-635-3429
adam.wehrenberg@cityofboston.gov

Kevin O'Shea
IE Division Information Security Practice Lead
New England Homeland Security Lead
URS Corporation
603-996-1826
kevin_oshea@urscorp.com

URS

NERCPI