Downtown Corridor Operation Crazy Train Cyber Tabletop Exercise After Action Summary Report

Overview

The RHPC's Downtown Corridor met on March 8th, 2018 to conduct a Tabletop Exercise (TTX) involving a cyber event affecting multiple agencies within the region.

A cyber event involving Hostage ware, Telephony Denial of Service (TDOS), and an overtaking of a facilities Computer Automated Facilities Management System was affecting various agencies in different ways across the corridor. Participants were introduced to an escalating scenario which allowed for both group and open discussions across multiple disciplines.

The following objectives were covered:

- Assess the preparedness of response staff to respond to and manage cybersecurity incidents.
- Test disaster recovery operations and procedures.
- Test internal and external processes for identifying and notification of cyber security incidents.
- Down time and Data Recovery procedures/operations.
- Determine the continuity of essential services.
- Identify the affected systems and the vulnerability of other systems.

Major Strengths

The major strengths identified during this exercise are as following:

1. Strong IT failure recovery planning
2. Connecting the training to Long Term Care agencies
3. Close partnership base for information sharing and organizational coordination.
4. Incident Command activation and involvement.
5. Downtime procedures and recovery planning.

Primary Areas for Improvement

Opportunities for improvement were identified as:

1. Information sharing should occur externally across the region to all partners.
2. Escalation Procedures, upline information sharing to include State and Federal levels.
3. Coordination of all agencies on current threats and dispersal of information.
4. Staff training to include phishing attacks.

Corrective Actions

The following Corrective Actions were identified:

1. Planning needs to occur across all channels, ensure your facilities plans are not constrictive in notification or reporting suspected or actual cyber incidents.
2. Develop additional training for End Users to include the inter-office use of Phishing Attacks.

Participating Agencies

The following agencies participated in the Tabletop Exercise:

1. The Medical Resort at Pearland
2. The Medical Resort at Bay Area
3. City of Houston, Homeland Security
4. Texas Children's Hospital
5. CHI St Luke's
6. Holly Hall
7. Diversicare Oakmont of Katy
8. MD Anderson Cancer Center
9. St Luke's Medical Center
10. Gulf Coast Regional Blood Center
11. Baylor St Luke's
12. Veterans Administration Hospital Houston
13. Memorial Hermann Health System
14. The Concierge
15. Harris Health
16. LBJ General
17. Texas Medical Center (HCPC)
18. St Joseph Medical Center
19. Ben Taub Hospital
20. VA Hospital OIT
21. HCA West Houston
22. The Women's Hospital of Texas (TWHT)
23. Courtyard Residence and Rehab Center
24. St Joseph Hospital
25. Memorial Hermann South West
26. Brazos Presbyterian Homes
27. Memorial Hermann Ambulatory