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

Overview

The RHPC's West 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. Established Systems and Policies.
2. Close partnership base for information sharing and organizational coordination.
3. Collaboration during the discussions provided for future partnership development amongst the players.
4. Command Center activation and involvement in cyber related issues.

Primary Areas for Improvement

Opportunities for improvement were identified as:

1. Information sharing should occur externally across the region to all partners.
2. Upline information sharing to include State and Federal levels.
3. Refinement of down-time procedures.
4. Reinforce training at all levels and continue to run phishing attack exercises.
5. Identifying a trigger system within the IT work order entry system.

Corrective Actions

The following Corrective Actions were identified:

1. Update plans to ensure information sharing across multiple agencies.
2. Identify needed Down Time Forms and ensure kits are developed for maintaining traditional records.
3. Incorporate trigger points into the planning process for notifying internal and external stakeholders.

Participating Agencies

The following agencies participated in the Tabletop Exercise:

1. Memorial Hermann Cypress
2. Kingwood Medical Center
3. Windsor Houston
4. Tomball Regional Medical Center
5. St Luke's The Vintage
6. Memorial Hermann MC
7. CRMC
8. First Texas Hospital
9. Huntsville Memorial Hospital
10. CHI St Luke's The Woodlands
11. Colonial Belle Nursing Home
12. Harris County Office of Emergency Management
13. Kindred Rehab Clear Lake
14. Diversicare
15. Heights N. Houston
16. Memorial Hermann Katy
17. Memorial Hermann Health System
18. Medical Resort at Sugar Land
19. Medical Resort at Willowbrook
20. Brazos Towers and Bayou Manner
21. Afton Diversicare
22. Oakmont Humble Diversicare
23. Memorial Hermann Memorial City
24. Conroe Regional
25. Montgomery County Health District
26. Cornerstone Conroe
27. Harris County Public Health (HCPH)
28. Texas Children's
29. Memorial Hermann Home Care
30. Texas Health and Human Services (DADs)

31. The Medical Resorts
32. TMR Sugar Land
33. LHS
34. North Cypress Medical Center
35. Brazos Presbyterian Homes
36. Tomball Rehab and Nursing
37. Health South Rehab Hospital The Woodlands
38. Regency Village
39. HCA Healthcare
40. West Janisch Health Care center
41. City of Houston
42. Kindred Rehab Hospital NE Houston
43. Lawrence Street Health Care Center
44. SETRAC