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

Overview

The RHPC's South Corridor met on March 9th 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. Information sharing and organizational coordination.
2. Collaboration during the discussions provided for future partnership development amongst the players.
3. Education and awareness.

Primary Areas for Improvement

Opportunities for improvement were identified as:

1. Information sharing should occur externally across the region to all partners.
2. Communication Plans need to be revisited to ensure completeness in addressing a cyber event.
3. Develop a better awareness of the external threats and the ability to function without technology for an undetermined period.
4. IT Back-up and downtime procedures.

Corrective Actions

The following Corrective Actions were identified:

1. Update plans to broaden the limits of cyber events and the agencies to coordinate with.
2. Identify needed Down Time Forms and ensure kits are developed for maintaining traditional records, include training on the use of these forms.
3. Incorporate additional cyber training in Employee Orientation and establish inter facility capability of testing Phishing on staff members.

Participating Agencies

The following agencies participated in the Tabletop Exercise:

1. Memorial Hermann
2. West Houston Rehab
3. Surgery Specialty Hospitals
4. Memorial Hermann Pearland
5. HCA Clear Lake
6. Memorial Hermann Sugar Land
7. HCA Mainland
8. Home Health Unlimited
9. Memorial Hermann South East
10. Clear Lake Regional Medical Center
11. St Luke's Sugar Land
12. Tuscany Village SNF
13. Houston Methodist Sugar Land
14. Clarewood House
15. Fort Bend County Health and Human Services
16. CHI St Luke's Patients Medical Center
17. OakBend Medical Center Jackson Street
18. OakBend Medical Center Williams Way
19. Houston Methodist St John's Hospital
20. Bay Wind Village Care Center
21. SPJ ST Senior Living Nursing Home
22. University of Texas Medical Branch Galveston
23. Cambridge H&R
24. West Houston Rehab
25. Mainland Medical Center
26. Pathways Memory Care
27. Ashton Parke Care Center

28. MRC The Crossing
29. Cypress Woods Care Center
30. LaVita Belle
31. Davita Dialysis
32. Tru Care Hospice
33. SETRAC