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

Overview

The RHPC's East Corridor met on March 6th, 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.
4. Downtime processes and back-up.
5. Redundancy of systems.

Primary Areas for Improvement

Opportunities for improvement were identified as:

1. Information sharing should occur externally across the region to all partners.
2. Continuity of Operations Plans need to be reviewed to ensure cyber incidents are addressed.
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.
5. Develop additional IT contacts within and outside the region to include higher levels of the government.

Corrective Actions

The following Corrective Actions were identified:

1. COOP reviews and incorporate Cyber into the planning process.
2. Identify needed Down Time Forms and ensure kits are developed for maintaining traditional records.
3. 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 Center of SE TX
2. The Medical Center of SE TX Beaumont
3. Focused Care at Baytown
4. Windsong Care Center
5. Anahuac EMS
6. Houston Methodist San Jacinto
7. Chambers County Emergency Management
8. Acadian Ambulance
9. Baptist Hospital Beaumont
10. Huffman EMS
11. Fall Creek Rehab
12. Chambers County Health
13. Bayside Community
14. Summer Place
15. Altus Hospice
16. Regent Care
17. Vidor Health and Rehab
18. SETRAC