FEBRUARY 5 - 6 • LOS ANGELES, CA

# SMART PORTS

## (INFORMATION TECHNOLOGY)


**Brant Mitchell, CISSP, CEM**

**Director**
**Stephenson Disaster Management Institute**
**Louisiana State University**


AAPA

# IT Recovery in the State of Louisiana

Recent Cyber Attacks in Louisiana

- 7 School Systems - July 2019
- Parish Governments – August 2019 – January 2020
- Law Enforcement Agencies – August 2019 – January 2020
- Institute of Higher Education – August 2019
- State of Louisiana – November 2019
- Baton Rouge Community College – December 2019
- City of New Orleans – December 2019
- New Orleans Convention Center – January 2020
- ITI Technical College in Baton Rouge – February 2020

# Emergency Support Function 17

## 15 Emergency Support Functions (ESF)

1. **Transportation**
   Department of Transportation

2. **Communications**
   National Communications System

3. **Public Works and Engineering**
   U.S. Army Corps of Engineers

4. **Firefighting**
   Department of Agriculture/Forest Service

5. **Emergency Management**
   Federal Emergency Management Agency

6. **Mass Care, Housing, Human Services**
   Department of Homeland Security
   American Red Cross

7. **Resource Support**
   General Services Administration

8. **Public Health and Medical Services**
   Department of Health and Human Services

9. **Urban Search and Rescue**
   Federal Emergency Management Agency

10. **Oil and Hazardous Materials Response**
    Environmental Protection Agency

11. **Agriculture and Natural Resource**
    US Department of Agriculture/Department of the Interior

12. **Energy**
    Department of Energy

13. **Public Safety and Security**
    Department of Homeland Security/Justice

14. **Community Recovery, Mitigation, and Economic Stabilization**
    U.S. Small Business Administration

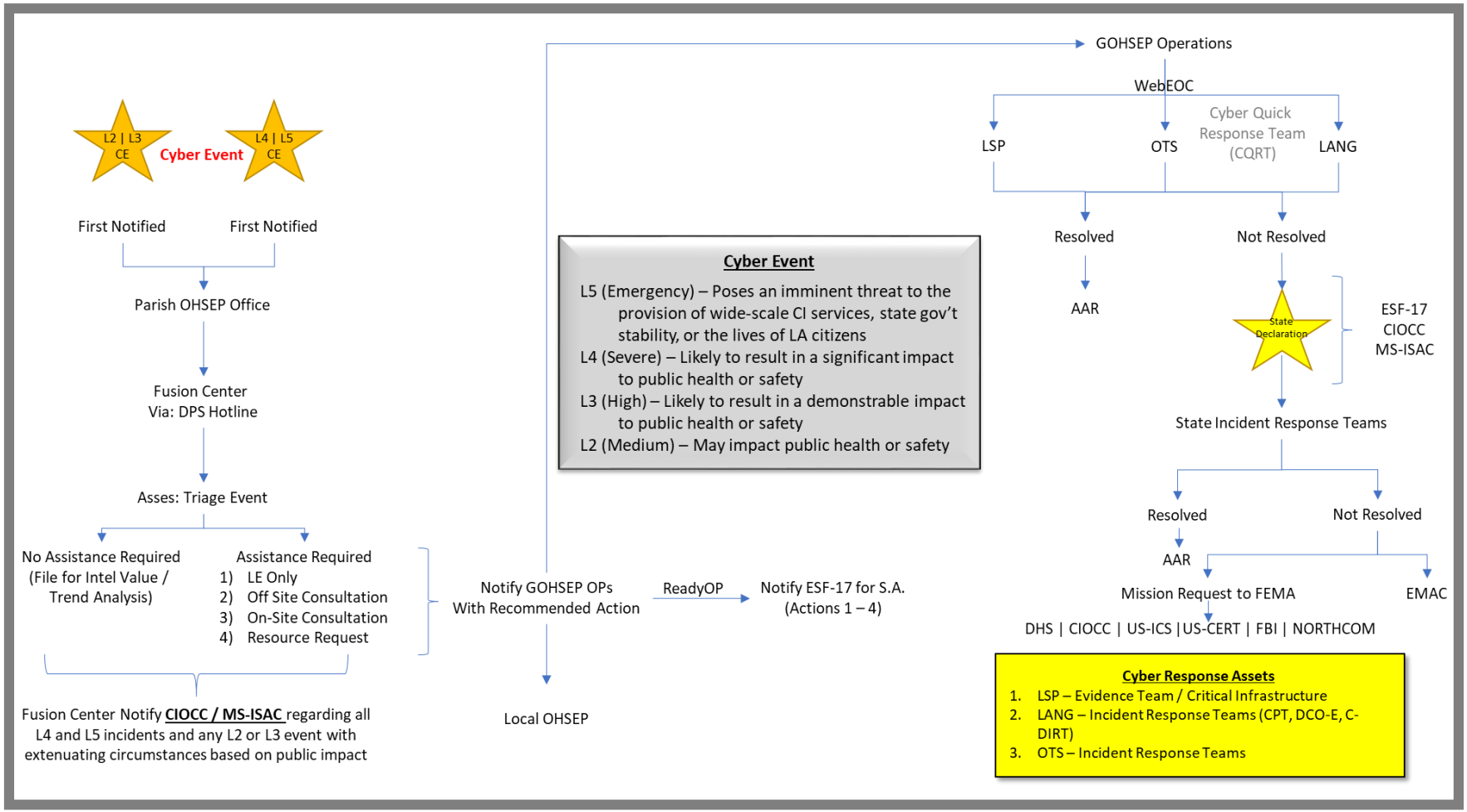
15. **External Communications**
    Federal Emergency Management Agency

# Ports in Louisiana




| | | | |
|---|---|---|---|
| 1 | Central Louisiana Regional Port | 17 | Port of Morgan City |
| 2 | Avoyelles Parish Port | 18 | Natchitoches Parish Port |
| 3 | Port of Greater Baton Rouge | 19 | Port of New Orleans |
| 4 | Port of Caddo-Bossier | 20 | Plaquemines Port |
| 5 | Port of Columbia | 21 | Port of Pointe Coupee |
| 6 | Port Fourchon | 22 | Red River Parish Port |
| 7 | Grand Isle Port | 23 | Port of South Louisiana |
| 8 | Greater Ouachita Port | 24 | Port of St. Bernard |
| 9 | Port of Iberia | 25 | Port of Terrebonne |
| 10 | Port of Krotz Springs | 26 | Port of Delcambre |
| 11 | Port of Lake Charles | 27 | Port of Vermilion |
| 12 | Port of Lake Providence | 28 | Port of Viadalia |
| 13 | Louisiana International Gulf Transfer Terminal | 29 | Port of Vinton |
| 14 | Madison Parish Port | 30 | West Calcasieu |
| 15 | Port Manchac | 31 | Cameron Parish Port |
| 16 | Port of Mermentau | 32 | Port of West St. Mary |

# Cyber Event Notification



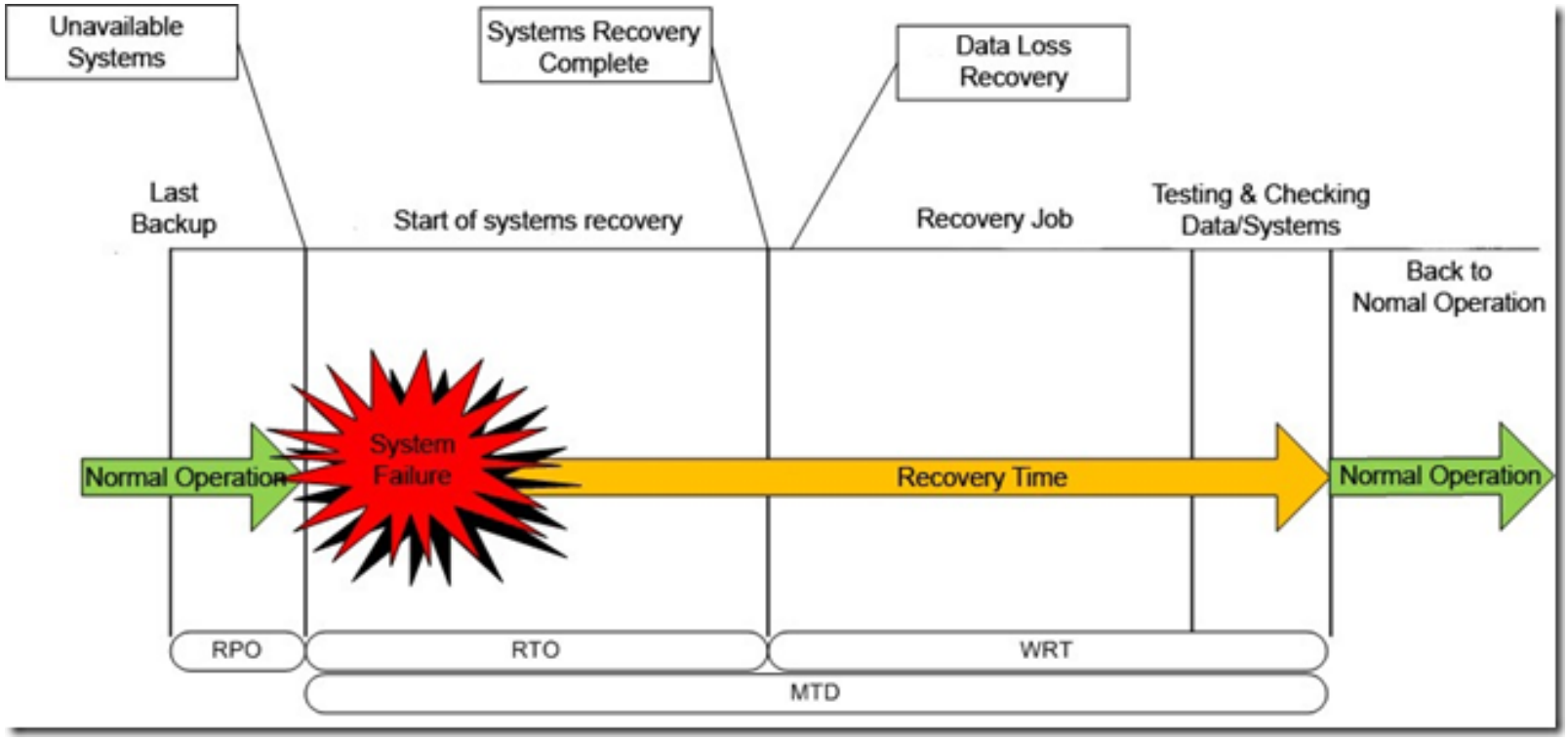
# Recovery Planning Considerations



| | Category | Self Assessed Current Profile | Assessed Current Profile | Target Profile |
|---|---|---|---|---|
| Identify | Asset Management (ID.AM) | Tier 1 | Tier 1.3 | Tier 3 |
| | Business Environment (ID.BE) | Tier 2 | Tier 2.2 | Tier 3 |
| | Governance (ID.GV) | Tier 1 | Tier 1.4 | Tier 3 |
| | Risk Assessment (ID.RA) | Tier 1 | Tier 1.3 | Tier 3 |
| | Risk Management Strategy (ID.RM) | Tier 1 | Tier 1.2 | Tier 3 |
| | Supply Chain Risk Management (ID.SC) | Tier 1 | Tier 1.5 | Tier 3 |
| Protect | Identity Management, Authentication and Access Control (PR.AC) | Tier 3 | Tier 2.4 | Tier 3 |
| | Awareness and Training (PR.AT) | Tier 2 | Tier 1.9 | Tier 3 |
| | Data Security (PR.DS) | Tier 1 | Tier 1.2 | Tier 3 |
| | Information Protection Processes and Procedures (PR.IP) | Tier 2 | Tier 1.9 | Tier 3 |
| | Maintenance (PR.MA) | Tier 2 | Tier 1.7 | Tier 3 |
| | Protective Technology (PR.PT) | Tier 2 | Tier 1.9 | Tier 3 |
| Detect | Anomalies and Events (DE.AE) | Tier 1 | Tier 1.7 | Tier 3 |
| | Security Continuous Monitoring (DE.CM) | Tier 2 | Tier 1.9 | Tier 3 |
| | Detection Processes (DE.DP) | Tier 1 | Tier 1.6 | Tier 3 |
| Respond | Response Planning (RS.RP) | Tier 1 | Tier 2.0 | Tier 3 |
| | Communications (RS.CO) | Tier 1 | Tier 1.2 | Tier 3 |
| | Response Analysis (RS.AN) | Tier 2 | Tier 1.7 | Tier 3 |
| | Mitigation (RS.MI) | Tier 2 | Tier 1.9 | Tier 3 |
| | Improvements (RS.IM) | Tier 1 | Tier 1.8 | Tier 3 |
| Recover | Recovery Planning (RC.SP) | Tier 2 | Tier 2.0 | Tier 3 |
| | Improvements (RC.IM) | Tier 2 | Tier 2.0 | Tier 3 |
| | Communications (RC.CO) | Tier 1 | Tier 2.1 | Tier 3 |

# Recovery Planning Consideration

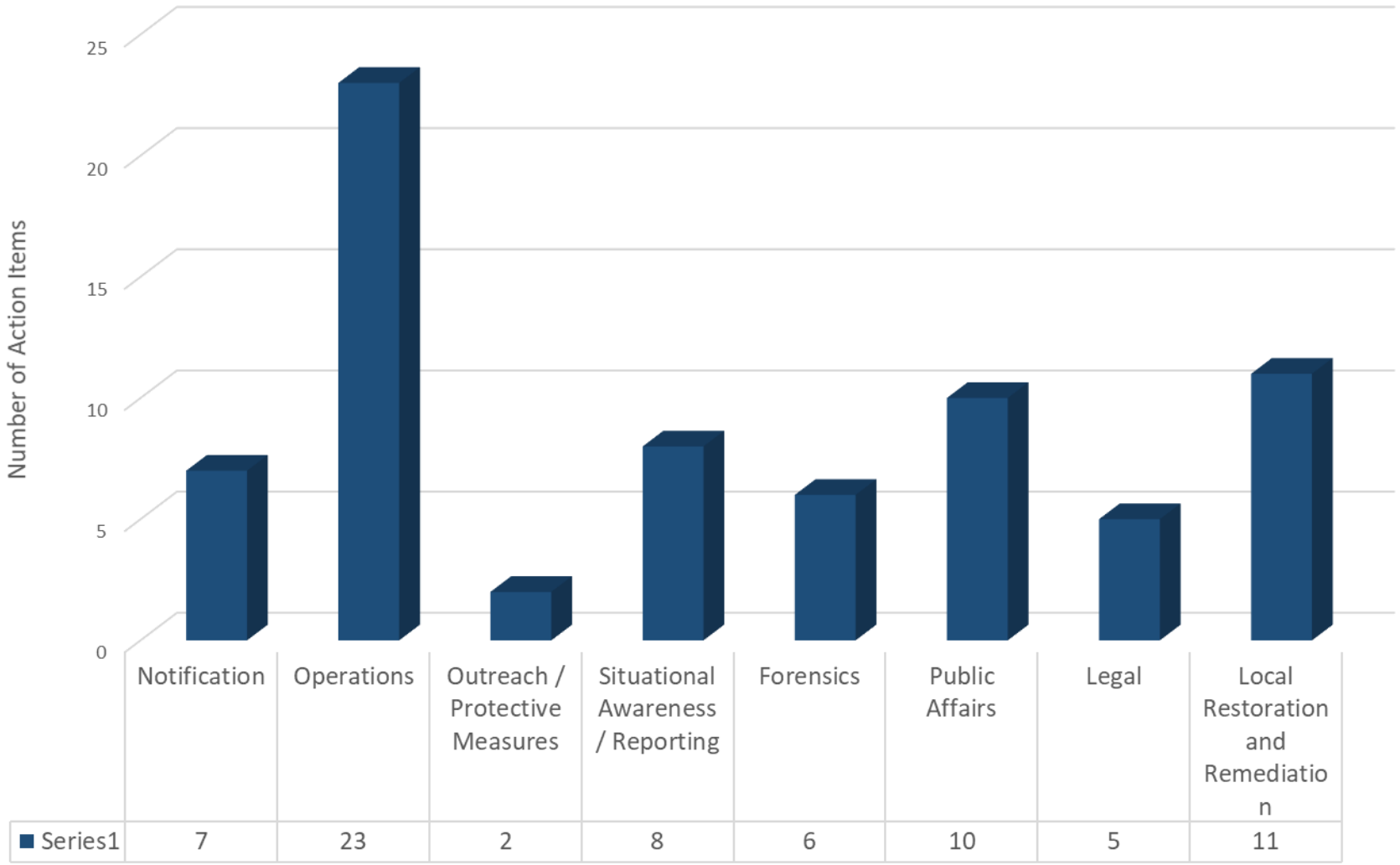
- Identify Work Functions that Require IT
- Identify Criticality of Each Function
- Identify Maximum Tolerable Downtime



# Ryuk Ransomware After Action Report



## Findings by Major Category



# Ryuk Ransomware Lessons Learned



- You need to have a plan
- Machines that were compromised had Local Admin privileges
- Do not re-image an impacted machine until forensics can be captured
  - Live Memory
  - Allows remediation course of action development
- Backups were not segregated from the network
- Test your ability to recover your data
  - Legacy Systems

# Ryuk Ransomware Lessons Learned



- Establish short-term and long-term recovery goals
  - Prioritize systems
- Provide your employees with cyber awareness training
- Your Public Affairs personnel need to have a base knowledge on cybersecurity
- Develop a reporting format to keep senior management informed
- Need to remove the stigma of being a victim of a cyber attack

# What You Can Do



- Develop, Update and Test Your Recovery Plan
- Identify Critical IT Functions and Establish Priorities of Effort
- Know What Resources are Available to You
  - State
  - Federal
- Get Involved
  - InfraGard
- Make Cybersecurity Part of the Organizations Culture