

**2026
DEFENSE HEALTH INFORMATION
TECHNOLOGY SYMPOSIUM**

**AUGUST 11-13, 2026
HYATT REGENCY NEW ORLEANS
NEW ORLEANS, LA**

IT Disaster Recovery - Leading MTFs Through IT Crisis

Luis Ofray, J-6 Academy Deputy Chief

LT USN Arion J McCartney

Gautham Ravichandran, PMP



UNCLASSIFIED

Agenda

1 Importance to Chief Information Officers (CIOs)

2 5 Phased Approach

3 Scenario

4 Key Takeaways

Speaker Introduction



Luis Ofray
J-6 Academy Deputy Chief

CIO J-6
Defense Health Agency



LT USN Arion J McCartney
Chief

Global Service Operations
Defense Health Agency



Gautham Ravichandran
Consultant/Trainer

CIO J-6
Defense Health Agency

Learning Objectives

- 1** Why ITDR Matters
- 2** CIO's Role in a Crisis
- 3** A Phased Approach to Disaster Recovery
- 4** Application of Phases to Scenario
- 5** Key Takeaways

The Stakes: Why This Matters

In a Military Treatment Facility, **IT failure equals clinical risk.**

- **Impacts:** Patient safety, mission readiness, and command trust.
- **What is a Disaster?**
 - Natural events (fires, floods, hurricanes)
 - Infrastructure failures (power, HVAC, network)
 - Cyber incidents (ransomware, insider threats)
 - Connectivity loss (WAN/DISA)
 - Mass casualty events or facility evacuations
- **Key Truth:** Disasters are not *if*—they're *when*. Most are compound events.

The CIO's Role in a Crisis: Leader, Not Technologist

During a disaster, your role transforms. You are the:

- **Advisor to Command:** Translating technical risk into clinical impact.
- **Decision Authority:** Making critical calls under pressure.
- **Cross-Domain Leader:** Aligning IT with Facilities, Cyber, and Clinical leadership.
- *Hesitation compounds damage. Your primary accountability is to document patient impact and drive change based on lessons learned.*

A Phased Approach to Disaster Recovery

A structured execution plan is key to managing a crisis effectively.

Prepare → Respond → Recover → Restore → Learn

Preparation: Planning decides outcome

Response & Activation: What happened and who needs to know?

Recovery & Resumption: How do we get back to work safely?

Restoration & Reconstitution: How do we return to normal operations?

Lessons Learned: How do we secure funding and improve for next time?

Preparation

Outcomes are determined before the disaster strikes.

- **Business Impact Analysis (BIA):** Identify Mission Essential Functions (MEFs) and define RTOs/RPOs.
- **Identify Clinical "Crown Jewels":** Prioritize systems like EHR/MHS GENESIS, PACS, Pharmacy, and Lab.
- **Infrastructure Reality Checks:** Assess power, network survivability, failover plans, and device dependencies.
- **Establish Order of Succession:** Who leads if you can't?

Response & Activation

The first 30 minutes are critical.

- **CIO Priorities:**
 - Analyze the situation.
 - Notify MTF Leadership immediately.
 - Establish command and control over the IT response.
 - Ensure personnel are safe.
- **Decision Framework:** Quickly decide—do we isolate systems or stabilize them?
- **Communication:** Communicate early and often. Use plain language. Silence creates panic.
 - Engage with MTF base comms early to get messaging to providers, beneficiaries, and leaders.

Recovery & Resumption

The focus shifts to safely restoring services.

- **Data Integrity First:** Validate data *before* restoring access. A fast recovery with bad data is a second disaster.
- **Prioritized Recovery Sequence:**
 - Identity & Access Management
 - Core Clinical Systems (EHR, PACS)
 - Ancillary Clinical Systems
 - Administrative Systems

Restoration & Normalization

The CIO's role in returning to a steady state.

- **Verify System Integrity:** Confirm root cause is mitigated and systems are stable.
- **Authorize Cutover:** Make the final "Go/No-Go" decision, owning the risk.
- **Conduct a Blame-Free Analysis:**
 - Did our technology meet RTOs and RPOs?
 - Which systems failed and which proved resilient? Why?
 - Where did our procedures or monitoring break down?

Lessons Learned & Continuous Improvement

Turn disaster analysis into funded action.

- **Report Upwards:** Brief executive leadership on the incident's impact, the corrective actions taken, and the investments required to strengthen IT resilience.
- **Translate Findings into Action:** Convert AAR findings into a concrete IT infrastructure Improvement Plan.
- **Update the DRP:** Mandate and approve all updates to plans, checklists, and diagrams.
- **Stay Prepared:** conduct joint tabletop exercises. Review annually.

Scenario

- During routine maintenance in the enterprise data center, a worker accidentally breaks a fire sprinkler head. Water pours directly onto the primary and secondary core network routers, destroying them instantly. This single event triggers an immediate, campus-wide network outage.

What Went Wrong? (Apply The 5 Phases)

- Facilities and Housekeeping departments refused to handle the water cleanup. Housekeeping stated it was outside their contract, while Facilities was unprepared.
- Once Facilities took responsibility, they discovered they could only authorize a small amount for an emergency cleanup contractor. Exceeding that limit requires a formal contracting process that would take days, not hours.
- A request to shut off the water immediately to mitigate damage was denied. Protocol dictated that only the Fire Department could authorize a water shutdown.
- The emergency power-off meant the uninterruptible power supplies (UPSs) did not shut down gracefully. The organization's policy required the UPS vendor to be called onsite to safely restore power, adding a mandatory 4-hour response time *after* the room was declared safe.
- With all systems down, the standard methods for communication and accessing documentation (like network configurations stored on a server) were unavailable.

Key Takeaways & Resources

- **IT Failure is Clinical Risk:** Frame decisions in terms of patient safety.
- **Preparation Determines Outcomes:** A robust, tested plan is your most critical asset.
- **Leadership Over Technology:** In a crisis, your role is to advise, decide, and communicate.

Contact: For further training, contact the J-6 Academy at: dha.j6academy@health.mil.

Contact

Luis Ofray

Deputy Training Chief, J-6 Academy

✉ luis.c.ofray.civ@health.mil

Gautham Ravichandran

Consultant/Trainer J-6 Academy

✉ gautham.ravichandran.ctr@health.mil
dha.j6academy@health.mil

LT Arion J Mccartney

Chief, Global Service Operations

✉ arion.j.mccartney.mil@health.mil

**2026
DEFENSE HEALTH INFORMATION
TECHNOLOGY SYMPOSIUM**

AUGUST 11-13, 2026
HYATT REGENCY NEW ORLEANS
NEW ORLEANS, LA

Thank You!



UNCLASSIFIED