

2026
DEFENSE HEALTH INFORMATION
TECHNOLOGY SYMPOSIUM

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

Day in the Life of a Cyber Event in DHA: Bridging Cyber Defense & Clinical Mission Assurance

Mr. Davin Evans / Mr. David Eaton



Agenda

1. Foundational Framework & Governing Authorities
2. Zero Trust & Clinical Mission Assurance
3. The Emergence of an Incident: Sources & Signals
4. The ISSM Playbook (The First 15 Minutes)
5. The CIO's Decision Point: Risk-Based Containment
6. Recovery & The Post-Incident Virtuous Cycle

Speaker Introduction - Mr. Davin Evans



Mr. Davin Evans DHA CyOC Operations Lead

Mr. Davin Evans is the DHA CyOC Operations Lead within the Defense Health Agency's Risk Management Executive (RME) Division.

A decorated U.S. Army Veteran with over 25 years of IT experience, Mr. Evans brings a wealth of knowledge to his role. He holds two BS degrees in Network/Security Management and Healthcare IT.

Speaker Introduction – Mr. David Eaton



Mr. David Eaton

DHA CyOC Operations Tool Team Lead

Mr. David Eaton serves as the Tools Team Lead for the DHA CyOC, operating within the Defense Health Agency's Risk Management Executive (RME) Division.

With a career spanning more than two decades in the Department of Defense, Mr. Eaton is a seasoned cybersecurity specialist who delivers deep technical leadership in IT management and information assurance. He holds an advanced degree, earning his Master of Science in Management Information Systems with a concentration in Information Security.

Learning Objectives

- 1** Internalize cyber defense as a core pillar of warfighter medical readiness and clinical quality
- 2** Differentiate between localized network "events" and validated "incidents" managed by the CyOC
- 3** Master the on-site ISSM "First 15 Minutes" tactical checklist
- 4** Apply the CIO Risk-Based Decision Matrix to balance security risks against immediate patient care requirements
- 5** Operationalize a proactive Zero Trust posture by shifting from "checklists to check-ins"

Governing Authorities & Mandates: The "Why"



USCYBER COM

Establishes strategic
DoW cyberspace
defense directives



DCDC

Directs physical
defense /
operations of the
DODIN;
issues tippers



DHA J-6 CIO/RMED

Establishes policies
and compliance
frameworks for
the DHA



CyOC

Executes real-time
operational defense
and coordinates
incident responses
across enterprise



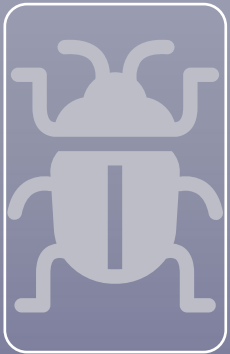
CSSPs

Provides deep
technical forensics,
malware analysis,
and adversarial
hunt capabilities



CyOC & CSSP Proactive Escalation Triggers

Malware Unauthorized Devices



Malicious Code Activity (Malware)

- *The Trigger:* EDR flags active ransomware staging, persistent Trojan beaconing, or credential harvesting tools on a clinical host.
- *The Call:* Immediate CyOC outreach to local ISSMs / SCARs to coordinate containment before lateral network spread occurs.

Sensitive Data Loss and DLP Triggers



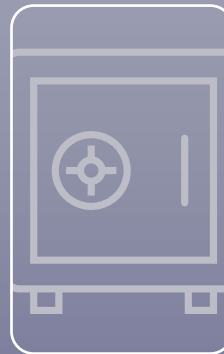
Data Loss and Exfiltration (DLP)

- *The Trigger:* Data Loss Prevention (DLP) sensors flag an anomalous bulk export of Protected Health Information (PHI) or Personally Identifiable Information (PII) to an unencrypted USB drive or unauthorized external email.
- *The Call:* CyOC contacts the ISSM/SCAR to halt the transfer, verify the clinical authorization of the user, and coordinate host isolation if a breach is suspected.



Unauthorized Access and Rogue Devices

- *The Trigger:* Network access controls detect an unapproved, unhardened personal laptop, rogue IoT device, or unauthorized wireless router connected to a Med-COI clinical switchport.
- *The Call:* CSSP flags the rogue MAC address and directs the local site to locate and physically remove the unauthorized hardware.



Coordinated Defense

- These triggers bypass normal ticketing queues. When CyOC / CSSP reach out regarding these events, they carry **direct technical containment recommendations** that require immediate local action.

Zero Trust Architecture as our Foundation



The Problem

Cybersecurity as a Compliance Hurdle

- Networks are vulnerable points of failure, risking care for warfighters and families.
- A single compromised endpoint can create a widespread impact across the entire network.



The Solution

Cybersecurity as a Mission Enabler

- A resilient network becomes the foundation for all critical capabilities (EHR, Telehealth).
- Zero Trust ensures a breach on one endpoint cannot move laterally, protecting patient care across the Med-COI.

The Emergence of an Incident: Sources & Signals

Detection Source: The WHO



Technical & Automated: SIEM, IDS, Firewalls, and EDR tools.



Strategic Partners: DCCDC Tippers, DC3, and Intel Agencies.



Proactive Hunt: CyOC/CSSP Threat Hunting, NWRT (Red Team) penetration tests.



Direct Reporting: User self-reporting, Insider Threat referrals.

Typical Event Types: The WHAT



Malicious Code: EDR flags unauthorized PowerShell activity on non-clinical asset.



Anomalous Activity: A user account logs in from an overseas IP at 3 AM.



Unauthorized Access: Rapid failed logins followed by a successful admin login.



Policy Violations: Data Loss Prevention / unauthorized software flags unencrypted PHI sent externally.

The ISSM Playbook: First 15 Minutes and Reporting

The “First 15 Minutes” Checklist

Acknowledge	Confirm call from CyOC / CSSP; obtain Master Ticket #.
Identify	Define the system's role (e.g., "Radiology station" or "ER kiosk").
Locate	Pinpoint physical building / room, IP, and Hostname.
Contact	Engage on-site system administrators and local support.
Brief	Give a concise, factual initial brief to your Site CIO.

Proactive Reporting (The 5 Ws)

Who	WHO is affected? (Users, departments, clinical systems)
What	WHAT was observed? (Ransomware splash screen, performance degradation)
Where	WHERE did it happen? (Physical room, IP address, building).
When	WHEN did it occur? (Exact timestamp, including time zone)
Witness	WITNESSES: Note any local IT staff or users who observed the event.

Phase 1 of 5: Detection & Validation *(Is it real?)*

The Event

EDR generates an alert for suspicious PowerShell activity on a clinical workstation at an MTF.

The Triage

CyOC/CSSP analysts cross-reference host telemetry with network and authentication logs.

The Declaration

Analysts confirm the activity is malicious, CSSP declares a formal incident, opens a master ticket, and alerts DCDC.

ISSM / CIO Role

None at this time.
Triage is kept internal to CyOC and NIWC CSSP to prevent false alarms and operational panic.

Phase 2 of 5: Notification & Coordination (*Command & Control*)

First Call

CyOC / CSSP calls the local ISSM with validated host details and recommendations.

Mission Context

ISSM provides immediate context back to the CyOC (e.g., "That workstation is the check-in terminal for the hospital visitor center").

Command Briefing

ISSM translates technical details into mission impact and briefs the Site CIO.

CIO Assessment

CIO evaluates operational impact and prepares clinical staff for potential downtime procedures.

The CIO's Decision Point: The Risk Matrix

Security Risk (CyOC Rated)	Low Mission Impact (ex: admin laptop, guest wi-fi)	High Mission Impact (ex: MHS Genesis, Radiology)
High Security Risk (active, spreading threat)	ACT DECISIVELY Upon receipt of a CyOC/CSSP isolation directive, the CIO signs off immediately. Security risk outweighs minor disruption.	CONSULT & DECIDE CyOC/CSSP issues urgent isolation directive. CIO rapidly coordinates with clinical leads and CyOC to transition to local Clinical COOP protocols before authorizing the disconnect.
Low Security Risk (contained, post-threat investigation)	CONTAIN & MONITOR CyOC/CSSP recommends logical containment. ISSM coordinates with CyOC to apply EDR logical isolation. Remediation is scheduled during a maintenance window.	SCHEDULED ACTION CyOC/CSSP recommends containment. CIO/ISSM coordinate with CyOC to delay physical disconnection/re-imaging until off-hours to preserve normal clinical operations.

Real-World Clinical Decision Scenario A



Active Threat / Radiology Imaging Suite

- **Threat:** EDR alerts show active lateral malware spread on a Radiology PACS terminal; CyOC/CSSP issues an urgent technical isolation directive for the local radiology subnet.
- **CIO Assessment:** High Security Risk / High Mission Impact.
- **Decision:** ACT DECISIVELY ON DIRECTIVE. CIO authorizes local execution of the CyOC / CSSP 's directive. Local IT disconnects the segment, and the Radiology department transitions to local Clinical COOP downtime protocols (e.g., local image caching and offline reading).
- **Rationale:** Preventing malware from spreading to the hospital's primary clinical and surgical networks outweighs the temporary local operational disruption within the Radiology suite.

Real-World Clinical Decision Scenario B



Post-Threat / Outpatient Check-in

- **Threat:** Forensic trace of a deactivated credential-harvesting tool found on a check-in kiosk; CyOC rates threat as Low Risk and issues a recommendation for timed logical containment.
- **CIO Assessment:** Low Security Risk / Medium Mission Impact.
- **Decision:** CONTAIN & MONITOR. Coordinate with the CyOC to apply a logical network block via the central EDR tool. Outpatient check-ins remain active under standard downtime procedures during peak hours.
- **Rationale:** Local leadership utilizes the CyOC's low-risk assessment to safely delay physical network disruption, preserving patient care while maintaining cybersecurity alignment. The kiosk's physical re-imaging is scheduled for off-hours (1700 hours).

Phase 3 of 5: Containment *(Stopping the Bleed)*

Technical Assessment

NIWC CSSP forensic telemetry recommends logical host isolation.

ISSM maps technical parameters to the clinical environment and briefs the CIO.

Risk-Based Decision

CIO approves containment action based on the Risk Matrix.

Per CyOC / CSSP direction, the ISSM directs local IT staff to physically disconnect the ethernet cable or apply the logical EDR network block.

Feedback Loop: ISSM confirms containment is complete back to the CyOC / CSSP.

CIO Talking Points: Communicating "Up & Out"

Executive Briefing Templates

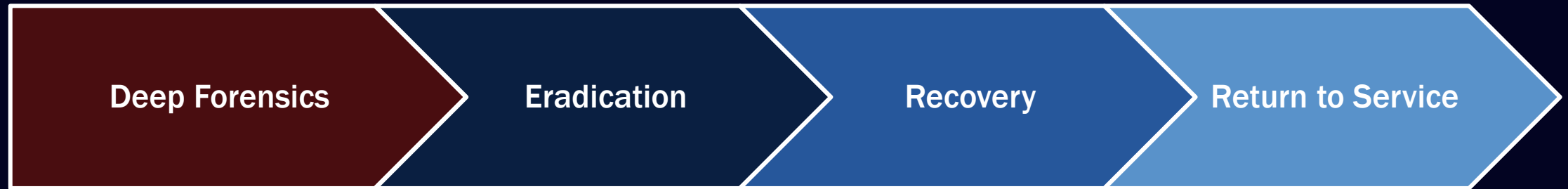
- The Opening: “We are actively managing a cybersecurity incident in close partnership with the DHA CyOC.”
- The Action: “Through collaboration with CSSP and CyOC, as a protective measure, we have temporarily taken [System Name/Function] offline to isolate and minimize the risk to our clinical network.”



Impact, Data, and Next Steps

- The Impact: “The operational impact is [e.g., slower check-ins at the front desk]. We have successfully transitioned to our established local Clinical COOP protocols to ensure uninterrupted patient care.”
- The Data: “Currently, there is no evidence that patient or personal data (PHI / PII) has been compromised. The technical investigation is active and ongoing.”
- The Next Step: “Technical teams are working to restore service safely. I will provide an update within [X] hours.”

Phase 4 of 5 - Eradication & Recovery *(Cleaning Up)*



NIWC CSSP performs forensic analysis on the isolated host to discover the root cause and sweeps the network segment for lateral movement.

Threat files are removed, and vulnerability mitigations are verified. CyOC issues the official "All Clear."

CIO, advised by the ISSM, authorizes restoration. Local IT re-images the workstation to guarantee a clean baseline.

Workstation is connected back to the Med-COI under DHA Zero Trust policies (comply to connect).

Phase 5 of 5: Post-Incident & Close-Out

CyOC Final Report

Prepares a detailed post-incident report (PIR) mapping the root cause, full timeline, and technical recommendations.

Master Ticket

The CyOC formalizes the close-out of the master ticket.

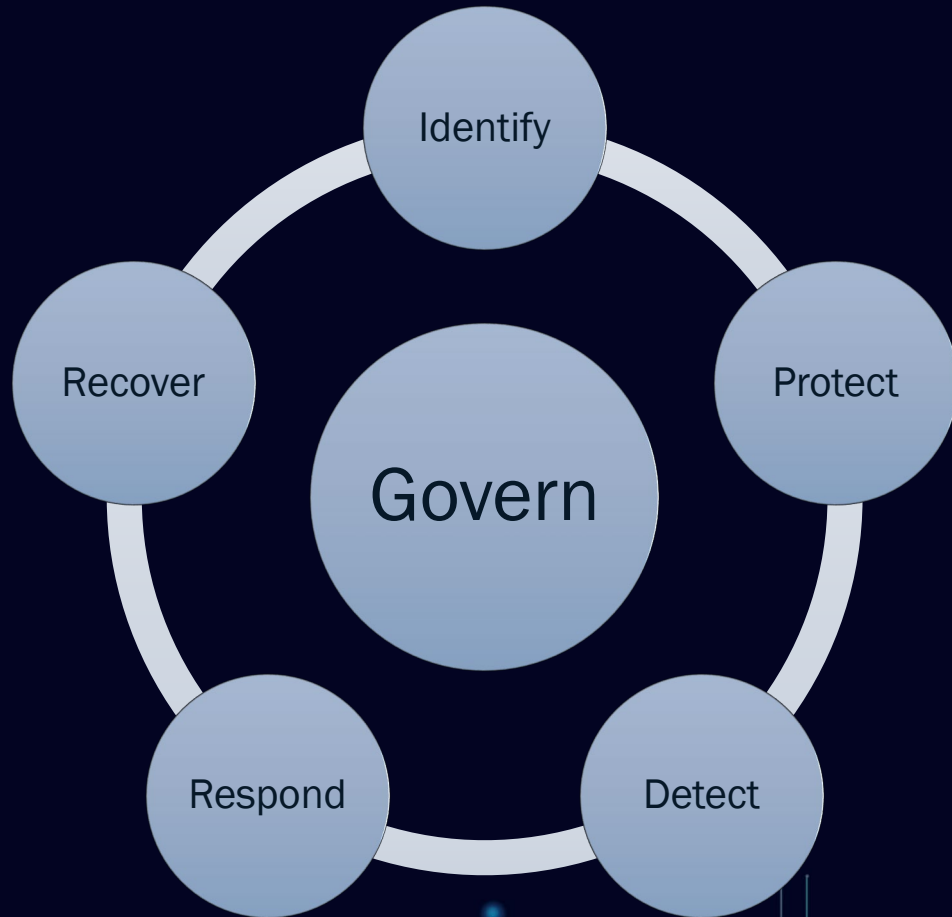
Local Retrospective

The ISSM conducts a local lessons-learned session with clinic leads to refine and update Clinical COOP and downtime procedures.

Strategic Action

The Site CIO uses the PIR data to drive future IT lifecycle investments, security awareness training, and network hardening.

The Call to Action: Shifting from "Checklists to Check-Ins"



Key Takeaways

- Cybersecurity is not an annual checklist; it is a continuous operational "check-in."
- By integrating CyOC defense, Red Team simulations, and clinical risk decisions, we build a truly resilient healthcare enterprise.

Connect with Our Team

Your Points of Contact for:

1. Event Response & Coordination
2. CSSP Coordination
3. Compliance Questions & Guidance
4. Technical Consultation
5. Higher Authority Tasking
6. Cyber Security Tool Compliance

Support You Need	Team to Contact	Email / Mailbox
Requests for Information	Action Officers	dha.jbcharleston.PEO-Med-Sys-J-6.mbx.cyoc-rfi@health.mil
Electronic Spillage	Event Response	dha.jbcharleston.peo-med-sys-j-6.mbx.cyoc-event-response@health.mil
Task Orders / Compliance	Compliance	dha.jbcharleston.j-6.mbx.compliance-team@health.mil
24/7/365 Watch Desk	DHA Global Service Desk	24/7/365 Help Desk 1.800.600.9332 https://gsc.health.mil/portal/index.cfm

Speaker Contact Profile



Mr. Davin Evans
DHA CyOC Operations Lead

✉ davin.j.evans1.civ@health.mil

Mr. David Eaton
DHA CyOC Operations Tools Team Lead

✉ david.z.eaton.civ@health.mil

**2026
DEFENSE HEALTH INFORMATION
TECHNOLOGY SYMPOSIUM**

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

Thank You!



UNCLASSIFIED