



 KAISER PERMANENTE.

Cyber Exercise

Network Outage June 7, 2024


Mitch Saruwatari, MPH: Director, National Emergency Management
Kimberly Galey, BS, EMT-P: Consultant, National Emergency Management

1

Presenter

Kimberly Galey
National Emergency Management Consultant
Kaiser Permanente

Kimberly Galey is a National Emergency Management Consultant with Kaiser Permanente. She supports the National Command Center (NCC) and national initiatives such as overseeing and shaping policies related to emergency management, providing ongoing education and regulatory survey support, partnering with internal and external stakeholders on emergency management projects and exercises, and leading and supporting groups focusing on planning, mitigation, response and recovery efforts.



2024 DISASTER PLANNING CONFERENCE | 2

2

Presenter

Mitch Saruwatari
Director of National Emergency Management
Kaiser Permanente

In this role, Mr. Saruwatari helps lead Kaiser Permanente in building resiliency through strategic planning, developing coordinated response activities and partnering in recovery capabilities resulting from any adverse event impacting health care delivery or business operations. Throughout his 25 years of emergency management experience, he has responded to many state and federal disasters including the September 11th Attacks, Hurricanes Katrina and Rita, multiple California Wildfires, Covid Pandemic, Ebola Outbreak. He has served on state and national committees including Chair for the Hospital Incident Command System (HICS) Center for Education and Training.



3

Disclosure of Relevant Financial Relationships

Kimberly Galey reports no relevant financial relationships or relationships she has with ineligible companies of any amount during the past 24 months.

Mitch Saruwatari reports no relevant financial relationships or relationships he has with ineligible companies of any amount during the past 24 months.



4



Today's Purpose: Test Your Cyber Resiliency in Real Time

Objectives:

- Learn the principles of conducting a cyber exercise in real-time using an actual network outage.
- Discuss lessons learned in planning and executing a cyber exercise.
- Identify opportunities to develop an outage-based exercise in your own organization.

5



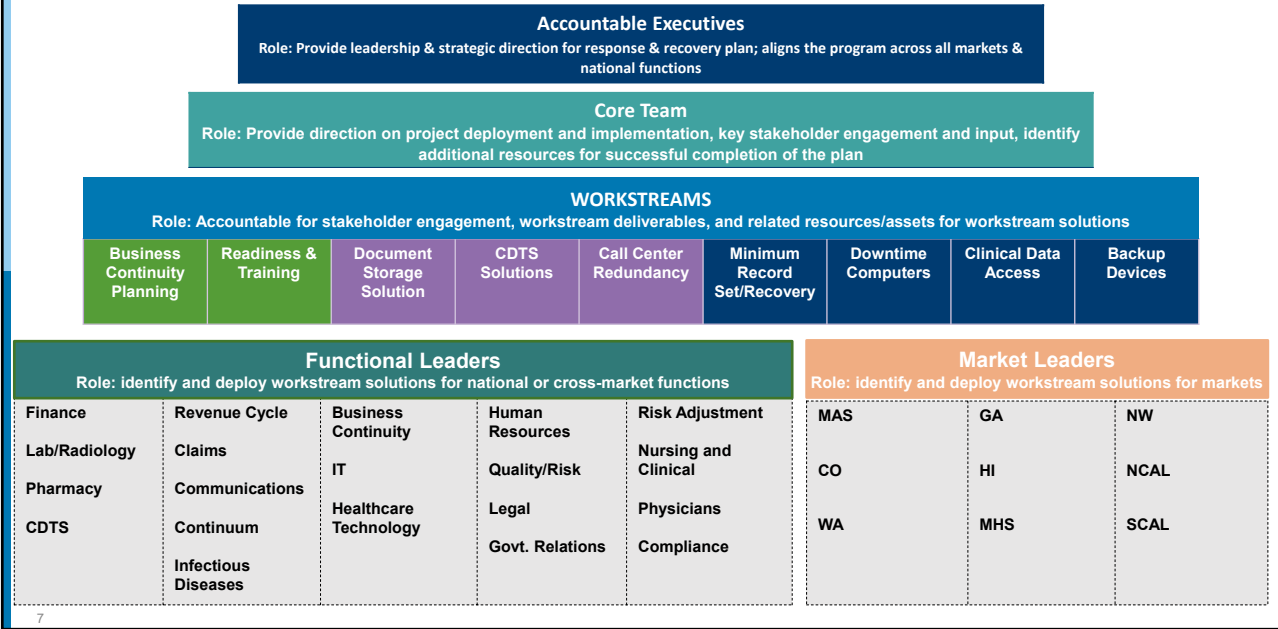
Overall Continuity Planning

- Establish an enterprise governance structure
- Identify critical business functions and services that need specific cyber security continuity plans
- Conduct business impact analysis
- Incorporate BIA/BCP in enterprise business continuity/disaster plans
- Train to the new standards and plans



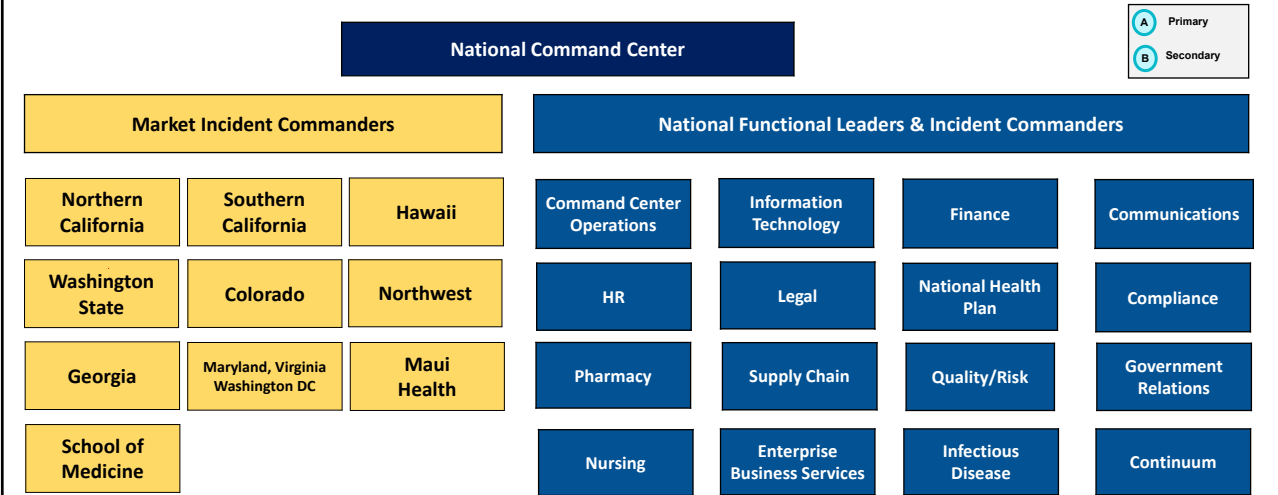
6

Governance Structure



7

National Command Center Structure



8

Exercise Goal and Scenario



Goal:

Test and validate Kaiser Permanente's readiness to respond to a cyber-attack causing a full network outage at a care delivery facility.

Scenario:

Rapidly spreading malware impacting select systems and network traffic in an outpatient care facility and dental office.

Exercise Objectives



Objectives:

1. Effectively Manage Operational Impacts
 - Impacted facilities will review, rehearse and implement Code Dark checklists, downtime procedures, and other outage strategies to support essential patient care services.
2. Implement Effective Command and Control Practices
 - Practice executing command-and-control to include activating National, Functional Areas, and Regional Command Centers, assembling appropriate response teams, and conducting Action Planning.
3. Coordinate Communication Activities
 - Test and evaluate communication processes, notifications, and alignment among response groups. Ensure consistent and unified messaging among all stakeholders.

Planning and Building the Exercise

First Steps:

- Success requires IT and Operations to carefully plan together
 - Shared and separate objectives
 - Master Scenario Events List, Exercise Plan, Exercise Evaluation Guide co-development
 - Use an actual outage, if possible
 - Stress your IT and Operational systems
- Exercise should be deployed like other exercises involving patient movement
- Requires a large number of players, evaluators, and volunteers
- May want to limit the number of observers
- Capture actionable lessons learned

11

Exercise Planning and Considerations

Planning began in January 2024

- Worked continuously with leadership at the National, Market and Local levels
- Site consideration and selection
- Planning meetings held weekly to coordinate the aspects of the exercise
- Regulatory and legal considerations
- Communications/Messaging
- Training
- Site set up



12

Site Selection – Outpatient Facility

Services:

- Reception
- Primary Care
- Wound Clinic
- Imaging
- Laboratory
- Pharmacy



Site Selection – Dental Office

Services:

- Reception
- Endodontist
- General Dentistry
- Oral Surgeon
- Orthodontist
- Pediatric Dentist
- Periodontist



Exercise Participants

Exercise Support

- Exercise Directors (2) – National Emergency Management and National IT Operations
- Exercise Controllers (2) – National Emergency Management
- Exercise Evaluators (10) – Delegates from other Markets, National Emergency Management, and National IT Operations
- Patient Actors (20) – Volunteer local managers and staff
- IT Support Staff (4) - To support the shutdown and restoration of systems

Exercise Players:

- National Command Center
 - Incident Commanders (2)- Health Plan and Physician Leader
 - Support Staff (2) – National Emergency Management, National Hospital Operations)
 - National Command Center Members (52)- Virtual and on site

Exercise Participants (cont.)

Exercise Players:

- KP Northwest Regional Command Center (14)
- IT Command Center (72 total. 25 in person and 52 virtual)
- Outpatient Facility Exercise Participants (38)
 - Clinicians, Department Managers and Staff
- Dental Office Exercise Participants (25)
 - Clinicians, Department Managers and Staff



Exercise Timeline

Time	Action
7:30 a.m.	IT Briefing
8:00 a.m.	IT portion of drill begins
11:45 a.m.	NCC activation
12:00 p.m.	Lunch is available for all attendees
12:00 - 12:30 p.m.	Attendees arrive at location and sign in
12:30 p.m.	Welcome and final briefing
12:50 p.m.	Move to exercise locations
1:00 p.m.	Clinical portion of exercise begins
4:30 p.m.	Clinical exercise concludes
4:30-5:00 p.m.	Clinical debrief concludes
5:00 - 6:00 p.m.	Dinner and exercise debriefing
6:30 p.m.	Exercise concludes

17

Activation Process

	Step	Lead	Comments
1	IT determines the situation and informs National Emergency Management (NEM) and National Command Center Incident Commander (NCC IC)	IT Incident Commander	Huddle/situation assessment with IT, NCC, and NEM
2	NCC IC leadership briefing	NCC ICs	NCC ICs (Health Plan and Physicians), NCC Command Center Operations Leaders
3	NCC leadership team makes decision to activate	NCC ICs	NCC IC directs NEM to send KP Alert to all NCC members. Message includes date/time
5	Hold first NCC briefing call	NCC ICs	Share situation, set meeting cadence and expectations for all members

18

Lessons Learned – What Worked



- Remote shutdown of impacted networks within 5 minutes as a malware containment strategy.
- Uninterrupted care to patients using Checklists and Plans.
- Deployed a read-only version of electronic medical record to allow clinicians to view patient history.
- Deployed alternate crisis response collaboration tools (offline documents and incident management platform).
- Utilized an alternate contact center solution which allowed agents to receive and route member calls.
- Rapidly deployed clean equipment to critical care delivery areas.
- Posted messages using alternate communication channels which allowed simplified external communications to members.

© 2023 Kaiser Permanente

Confidential, not for distribution or duplication

page 19

19

Lessons Learned - Opportunities



- Some clinicians were unable to access the read only EMR backup.
- Consider improvements for remote employees connecting to the network.
- Additional review needed of alternative communications solutions.
- Consider opportunities to enhance virtual care.
- Consider opportunities for consolidation of data recovery and reconciliation after a crisis event.
- Checklists and Plans require review and updates to include additional care delivery workflows.

© 2023 Kaiser Permanente

Confidential, not for distribution or duplication

page 20

20

What's Next?



Continue Building Resiliency Through Continuous Improvement

- Capture lessons learned from exercises and real events.
- Identify actions and implement changes to policies and practices.
- Keep cyber security knowledge current.
- Validate changes to plans and technology through testing and exercises.
- Constant vigilance. Keep cyber security top of mind for everyone in the organization through communications, reminders and testing.



2024 DISASTER PLANNING CONFERENCE **PASADENA**

Questions?



 California Hospital Association

Thank you!

Kimberly Galey

National Emergency Management Consultant
Kaiser Permanente
Kimberly.C.Galey@kp.org

Mitch Saruwatari

Director of National Emergency Management
Kaiser Permanente
Mitchell.W.Saruwatari@kp.org

