

Healthcare Facility Business Continuity Plan Tabletop Exercise:

Cyber Attack

Situation Manual

[Exercise Date]

*This document was last updated 12/28/16*

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. All participants may view the SitMan.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Healthcare Facility Business Continuity Plan Tabletop Exercise: Cyber Attack |
| **Exercise Dates** | [Enter Date and Time] |
| **Scope** | This tabletop exercise is planned for [Enter Time] at [Enter Location and Address] to test, evaluate and validate the [Hospital Name and/or Department Name] Business Continuity Plan. Exercise play is limited to the presentations and discussions held by exercise participants. Participants will include representation from *Administration, Emergency Management, Finance, Human Resources, Information Solutions, Marketing and Communications, Nursing, and Plant Operations/Maintenance*  [Use interdependencies to determine who the Participants should be]. |
| **Mission Area(s)** | Response and Recovery |
| **Core Capabilities** | 1. Emergency Operations Coordination/Hospital Command Center Management 2. Communications and/or Information Gathering & Intelligence 3. Business/Healthcare Continuity |
| **Objectives** | 1. Activate and use Incident Command System (ICS) principles (ICS, Hospital Incident Command System, and Standardized Emergency Management System) across all levels of the medical and health system. 2. Information/intelligence gathering. 3. Evaluate the ability to use existing systems to communicate. 4. Validate Business Impact Analysis (BIA) and Business Process Analysis (BPA). 5. Test the effectiveness of continuity and recovery strategies to continue specific operations 6. Identify trigger points for establishing the need or process for relocation. |
| **Threat or Hazard** | Cyber Attack. |
| **Scenario** | An attack affecting or disrupting critical infrastructure elements and electronic medical records, intended to disrupt certain elements of critical infrastructure, information solutions, and organizational economic and financial structures. |
| **Sponsor** | This exercise is sponsored by the Los Angeles County Emergency Medical Services Agency. The exercise is funded by grant number: 5U90TP000516-02. |
| **Participating Organizations** | [Enter Name of Hospital and other organizations participating in the tabletop exercise] |
| **Points of Contact** | [Name of Facilitator] [Title]  [Facility Name]  [Facility Street Address] [Facilitator Email]  [Facilitator Phone]  [Additional POCs - Name]  [Title]  [Facility Name]  [Facility Street Address] [Facilitator Email]  [Facilitator Phone] |

# General Information

## Exercise Objectives and Core Capabilities

The scenario focuses on the organizations ability to coordinate and implement prevention, preparedness, response and recovery plans and capabilities pertaining to a significant cyber event or a series of events. The following exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to core capabilities, which are distinct critical elements necessary to achieve the specific mission area(s). The following objectives and capabilities have been selected by the Los Angeles County EMS Agency Healthcare Continuity and Recovery Workgroup. They are based on the National Preparedness Goal (NPG) and ASPR Health Care Preparedness and Response Capabilities. These capabilities provide the foundation for development of the exercise objectives and scenario. The purpose of this exercise is to measure and validate performance of these capabilities and their associated critical tasks. The following table details the objectives and associated selected capabilities.

Table 1. Exercise Objectives and Associated Core Capabilities

|  |  |  |
| --- | --- | --- |
| Exercise Objective | National Preparedness Goal (NPG)  Capability | ASPR  Capability |
| 1. Activate and use Incident Command System (ICS) principles (ICS, Hospital Incident Command System, and Standardized Emergency Management System) across all levels of the medical health system. | **Operational Coordination** | Healthcare and Medical Response Coordination |
| 1. Information/Intelligence gathering. | **Intelligence and Information Sharing**  **Situational Assessment** | Health Care and Medical Response Coordination |
| 1. Evaluate the ability to use existing systems to communicate. | **Situational Assessment**  **Operational Communications** | Healthcare and Medical Response Coordination |
| 1. Validate Business Impact and Business Process Analysis. | **Risk and Disaster Resilience Assessment**  **Infrastructure Systems**  **Economic Recovery** | Continuity of Health Care Service Delivery |
| 1. Test the effectiveness of recovery strategies to continue specific operations. | **Infrastructure Systems**  **Economic Recovery** | Continuity of Health Care Service Delivery |
| 1. Identify trigger points for establishing the need or process for relocation. | **Infrastructure Systems**  **Economic Recovery** | Continuity of Health Care Service Delivery |

## Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

* **Players.** Players are personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
* **Observers.** Observers do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
* **Facilitators.** Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
* **Evaluators.** Evaluators are assigned to observe and document certain objectives during the exercise. Their primary role is to document player discussions, including how and if those discussions conform to plans, polices, and procedures.

## Exercise Structure

This exercise will be a multimedia, facilitated exercise. Players will participate in the following three modules:

* Module 1: Initial Incident Actions and Mitigation
* Module 2: Incident Response
* Module 3: Incident Resolution, Recovery and Continuity of Operations

Each module begins with Scenario Background or Scenario Update that summarizes key events occurring within that time period. After the background/updates, participants review the situation and engage in functional group discussions of appropriate response issues. For this exercise, the functional groups are as follows: [As outlined above, determined by interdependencies].

* Administration
* Emergency Management
* Finance
* Human Resources
* Information Solutions
* Marketing and Communications
* Nursing
* Plant Operations/Maintenance

After these functional group discussions, participants will engage in a moderated plenary discussion in which a spokesperson from each group will present a synopsis of the group’s actions, based on the scenario.

## Exercise Guidelines

* This exercise will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected.
* Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
* Decisions are not precedent setting and may not reflect your organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.

Issue identification is not as valuable as suggestions and recommended actions that could improve response efforts. Problem-solving efforts should be the focus. Information gathered during this exercise will be reviewed to assess modification to the relevant Business Continuity Plan.

## Exercise Assumptions and Artificialities

In any exercise, assumptions and artificialities may be necessary to complete play in the time allotted and/or account for logistical limitations. Exercise participants should accept that assumptions and artificialities are inherent in any exercise, and should not allow these considerations to negatively impact their participation. During this exercise, the following apply:

* The exercise is conducted in a no-fault learning environment wherein capabilities, plans, systems, and processes will be evaluated.
* The exercise scenario timeline will be accelerated to test the exercise objectives. Triaging and coordination of patient destination would take a considerate amount of time in this scenario.
* All players receive information at the same time.

## Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned capabilities, capability targets, and critical tasks, which are documented in Exercise Evaluation Guides (EEGs). Evaluators have EEGs for each of their assigned areas. Additionally, players will be asked to complete participant feedback forms. These documents, coupled with facilitator observations and notes, will be used to evaluate the exercise and compile the After-Action Report (AAR).

# Module 1: Initial Incident Actions And Mitigation

### Scenario Background: September 29, 2016 / 0800 hrs.

A report on planned hacktivist actions against U.S. interests has been received from The Void, and the report was confirmed by various cyber security firms. The report is specific to the Health Sector.

## Key Issues

* Preventive measures/mitigation
* Situation assessment
* Decision making and authority

## Instructions

Based on the information provided, participate in the discussion concerning the issues raised in Module 1. Identify any critical issues, decisions, requirements, or questions that should be addressed at this time.

## Discussion

The following questions are provided as suggested subjects that you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

### Questions

1. Who would receive this information? Who would the information be communicated to?
2. Do we feel compelled to take any preventative measures?
3. How do variables in the threat information that we receive – such as timeframe, credibility, and specificity – impact our decision making and prevention efforts? Discuss the coordination efforts that would occur in this type of incident.
4. What tools do we use to support cyber prevention?
5. How do we share cyber threat information internally? How do we share information externally, with groups like law enforcement entities?
6. Do we feel compelled to activate our response plans, business continuity plans, or an incident management team (IMT)? If so, would it be just Information Solutions, or would it include representatives from other departments and leadership? Who should make up the IMT?

# Module 2: Incident Response

### Scenario Update: September 29, 2016 / 0900 hrs

For the past couple of weeks ago, our security event console indicated the detection of suspicious network activities. Our system administrator conducted his daily check on the system backup server and discovered a backup error message. Upon further investigation, he did not find any additional errors, nor did he notice anything unusual. The system administrator logged the error message according to our standard logging procedures.

One week ago, the database server on our corporate local area network crashed. After an automatic reboot, operations appeared normal, but shortly afterwards IT Support received several phone calls from users in the Accounting Department reporting that their network appeared to be slow. By noon that same day, additional calls were received from users in other departments, to the point where IT support became overwhelmed and considered escalating the problem to management.

One hour ago, we learned that our facility is The Void’s primary target, and they’re wreaking havoc on our company. They are illegally transferring our money, sending customers fraudulent invoices, and threatening extortion. They’ve also disabled our internal internet, impacting systems that we use to communicate with patients, providers and staff. Our computers are starting to lock out.

In addition to those internal issues, The Void’s hacking is having significant negative impacts on our business:

## Key Issues

* Detection.
* Resources.
* Downtime.
* Plans and policies.
* Communication to organization/customers.
* Service continuity.

## Instructions

Based on the information provided, participate in the discussion concerning the issues raised in Module 2. Identify any critical issues, decisions, requirements, or questions that should be addressed at this time.

## Discussion

As we move to the discussion part of this module, focus on the ways we would notify stakeholders and share information to combat this attack.

The following questions are provided as suggested subjects that you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

At this point, the most important questions that we need to address are:

**Communication Issues**

1. What internal and external messages would need to be developed? How are the messages being distributed? Who leads the public information process?
2. What about planned notifications? How do we do this internal and external to our organization?

**Cyber Issues**

1. How would we/how would you detect malicious activity of unknown origin on our systems? What are our top priorities at this time?
2. How would we/how would you quickly respond to a suspected cyber attack? How are decisions made about protecting the system/data versus investigating this problem as a crime? Who makes the decision?
3. What tools or assets do we have/do you have to assist in detecting unauthorized activity?
4. What type of detection hardware and/or software do we use? How successful or unsuccessful has this software/hardware been in detecting and/or preventing this activity?
5. How would we/how would you conduct an assessment of this situation?
6. What resources do we have or could we request for network forensics?
7. Where do we receive our cyber response technical assistance?
8. Do we have plans, procedures or policies in place to access this assistance?
9. What are the needed resources and where would we get them?
10. Do our current mutual aid agreements address cyber specific resources and staff?
11. Do we have a Cyber Incident Response Team? What is their composition/skill set?

**Additional Response Considerations**

1. At what point do we contact law enforcement? Who makes contact, and who do we contact?
2. What are the business implications of the scenario? How would we determine them, e.g. brand, reputation or financial impact?
3. Are IS/IT and business continuity functions coordinated with physical security? Would all three then be collaborating with public relations, human resources, and legal departments? Would we activate HICS and the HCC?

# Module 3: Incident Resolution, Recovery And Continuity of Operations

### Scenario Update: November 24, 2016 / 1300 hrs.

## We’ve been at this for about many weeks now. It all started with a general threat warning issued by The Void, saying that they’d be attacking U.S. interests with “zero day” attacks. Then, our organization conducted a security audit that uncovered a terminated employee with system access. A week later, an employee found a USB drive in the parking garage and proceeded to use it. Unbeknownst to the employee, the USB drive was used by The Void to create a backdoor into our networks.

## Things started to fall apart from here, as our employees started receiving and opening phishing emails from The Void, the database server crashed resulting in a slow network and slow productivity; several illegal transfers of our money were made; and false invoices were distributed to a number of our clients. And it didn’t stop there. To add insult to injury, the hackers sent an email indicating that the company’s network had been infiltrated and various components taken over; threatened to cripple the company’s network and expose proprietary company data unless they received $1 million; and, finally, brought our website down, crippling our ability to communicate with each other and our customers.

## Thankfully, through close collaboration with law enforcement and security consultants, we were able to stop the attack, but not before it caused significant damage to our business, in the form of loss of census/patient admitting, as well as market share and profit losses. The community didn’t have faith that their records would be kept confidential.

## Instructions

## Based on the information provided, participate in the discussion concerning the issues raised in Module 3. Identify any critical issues, decisions, requirements, or questions that should be addressed at this time.

## Discussion

The following questions are provided as suggested subjects that you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

**Questions**

1. If our organization is disconnected from its network access during the cyber attack, what procedure would we use to restore connectivity?
2. What are the systems that should be prioritized first for repair or restoration?
3. How could we coordinate patient treatment with other health and medical providers, e.g. sister facilities, hospitals, surgical centers, long term care facilities, clinics?
4. Based on the information presented, what are our top priorities at this time?
5. What costs associated with our organization’s operations during the incident are reimbursable? How will reimbursement be obtained?
6. How are costs tracked? What records or paperwork is needed to do so?
7. How long will it take to recover the patient records if we were down for one month? How long will it take to bill those records? Is extra staff required?
8. What is the recovery strategy around the data center? Do we need to consider relocation?
9. How can we improve training programs so that we are better prepared for a cyber attack in the future? How do we prioritize these activities? What tools are available to help improve these activities?
10. How are interdependencies coordinated? Who should they be coordinated with?

# Appendix A: Exercise Schedule

| Time | Activity |
| --- | --- |
| **September 29,2 016** | |
| 1100 | Welcome and Opening Remarks |
| 1115 | Module 1: Briefing, Group Discussion, and Plenary Discussion |
| 1140 | Module 2: Briefing, Group Discussion, and Plenary Discussion |
| 1205 | Table Discussion |
| 1230 | Module 3: Briefing, Group Discussion, and Plenary Discussion |
| 1300 | Hot Wash |
| 1325 | Closing Comments  Completion of evaluations |

# Appendix B: Exercise Participants

* Administration
* Emergency Management
* Finance
* Human Resources
* Information Solutions
* Marketing and Communications
* Nursing
* Plant Operations/Maintenance

# Appendix C: Relevant Plans

* [Enter Relevant Plan Here]
* [Enter Relevant Plan Here]
* [Enter Relevant Plan Here]
* [Enter Relevant Plan Here]
* [Enter Relevant Plan Here]