Tabletop Exercise (TTX) – Hospital Ransomware Attack

Situation Manual

November 2022

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Tabletop Exercise (TTX) - Cyber |
| **Exercise Dates** | DATE Month/Day/Year |
| **Scope** | This exercise is a tabletop exercise. |
| **Mission Area(s)** | Prevention, Protection, Mitigation, Response & Recovery |
| **Core Capabilities** | Planning, Public Information and Warning, Operational Coordination |
| **Objectives** | This TTX was written with six (6) SMART objectives listed. Choosing which objectives, you as the sponsoring agency have the responsibility of picking which objectives better fit your agency’s needs. As a discussion-based exercise, participating agencies discuss practicing group problem solving, familiarizing senior officials with a situation, conducting a specific case study, examining personnel contingencies, testing group message interpretation, participating in information sharing and assessing interagency coordination. |
| **Threat or Hazard** | Cyber |
| **Scenario** | The Cyber TTX was designed around a realistic scenario. |
| **Sponsor** | PEMA/ GOHS/ Your Agency |
| **Participating Organizations** | Federal, state, tribal or local levels of government agencies while utilizing the whole community approach of including applicable representative organizations (such as private sector partners, voluntary agencies, school districts, etc.) within each jurisdiction. |
| **Point of Contact** | Your Information  General Inquires: Kamie Hughes: PEMA: Kamhughes@pa.gov |

# General Information

## Exercise Objectives and Core Capabilities

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 objectives and aligned core capabilities are guided by elected and appointed officials and selected by the Exercise Planning Team.

| Exercise Objective | Core Capability |
| --- | --- |
| Examine local government role in management of cascading events caused by cyber-attacks against public and private sector entities providing essential services. | Planning, Public Information and Warning, Operational Coordination |
| Increase local government awareness of issues and concerns related to public or private sector reporting of significant cyber incidents. | Planning, Public Information and Warning, Operational Coordination |
| Examine bi-direction federal, state, and local government cyber incident reporting and cybersecurity information sharing. | Planning, Public Information and Warning, Operational Coordination |
| Increase awareness of public and private sector cybersecurity preparedness efforts and incident response capabilities. | Planning, Public Information and Warning, Operational Coordination |
| Examine the process to coordinate public and private sector public notifications related to the impacts of reported significant cyber incidents | Planning, Public Information and Warning, Operational Coordination |
| Increase local government awareness of the role of the Pennsylvania Cyber Incident Annex in guiding state and local response to significant cyber incidents. | Planning, Public Information and Warning, Operational Coordination |

Table 1. Exercise Objectives and Associated Core Capabilities

## 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 Preparation:** *What is needed to get the most value out of this exercise?*

* Review the provided exercise objectives and add additional objectives that the county wishes to demonstrate.
* Develop discussion questions that are relevant to the objectives of the exercise. Discussion questions related to reported significant cyber incidents can be taken from the county ransomware exercise scenario that is also being provided by PEMA Division of Training & Exercises.
* Cut and paste the exercise injects and discussion questions into a PowerPoint presentation for display to participants during the tabletop exercise.
* Invited participants can include but are not limited to personnel from the county emergency management agency, 9-1-1 dispatch center, county Information Technology (IT) department, hospitals, emergency medical services, local law enforcement agencies, and other public and private sector emergency management and cybersecurity stakeholders.
* Identify an individual to present injects and solicit participant responses to the discussion questions.
* Assign one or two recorders to document participant-identified best practices, and organizational strengthens and weaknesses to facilitate completion of an after-action report and corrective action plan.
* Register participants and make up tent card displaying the participant’s name, title and organization.
* During the exercise, tent cards should be placed in front of participants facing the exercise facilitator to allow for identification of participants and job responsibilities. The facilitator does not need an IT background to help conduct this exercise.
* This exercise can be conducted virtually or in a hybrid format to meet the needs of the participants.
* Plans, procedures, policies, and other relevant documents should be provided to participants ahead of time for familiarization.

## 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 prevention/protection/mitigation/response/recovery efforts. Problem-solving efforts should be the focus.

## 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 is plausible, and events occur as they are presented.
* 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), where applicable. 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).

# BACKGROUND

Ransomware, which is used to extort its victims into paying large sums of money to retrieve their encrypted data, is a malicious form of cyberattack that has proven to be quite lucrative for cybercriminals when used against healthcare providers, who often pay the ransom to regain access to their data. These attacks can additionally result in the shutdown of medical equipment which hospitals rely to diagnosis and treat their patients

A real-world scenario for consideration, on September 11, 2020, a woman in Germany (referred to here as Patient X) died from an aortic aneurysm while being transported the approximately 20 miles from Düsseldorf to a hospital in Wuppertal. University Hospital Düsseldorf had to turn away the ambulance transporting Patient X because its whole IT network had been crippled by ransomware. Patient X is thought to be the first person whose death could possibly be attributed to a ransomware attack.

*Copyright Credit: Yale Cyber Leadership Form, Attributing Deaths to Ransomware Attacks on Hospitals and Medical Care Facilities, July 20, 2021 by Margaret House (YLS’22)*

**Inject 1 - <Insert Date and Time (Two weeks before Inject 3) >**

The Federal Bureau of Investigation (FBI) FLASH titled “Indicators of Compromise Associated with Hive Ransomware” **(TLP:WHITE // U/FOUO)** is forwarded by the Pennsylvania Criminal Intelligence Center (PaCIC) to provide situational awareness to their public and private sector cybersecurity intelligence subscribers about tactics, techniques and procedures (TTPs) of cyber actors using Hive ransomware.

The bulletin summary states that Hive ransomware actors exfiltrate data and encrypt files on a network. The actors leave a ransom note within the victim’s system which provides instructions on how to purchase the decryption software. The ransom note also threatens to leak exfiltrated victim data on the Tor site, HiveLeaks, if the ransom demand is not met.

Hive ransomware attackers are notorious for going after targets that other hackers intentionally avoid. These targets include physician offices, hospitals and health care systems.

*Copyright Credit: Federal Bureau of Investigation, Cyber Division*

**Inject 2 - <Insert Date and Time (Five days before Start) >**

An Intelligence Analyst in the New York State Intelligence Center (NY SIC) sends an e-mail to members of the Cyber Intelligence Network (CIN) to inform them that several hospitals in the same metropolitan area were victims of ransomware attacks.

The federal and state investigations associated with these cyber incidents is on-going; however, there is growing concern that these medical facilities were targeted by a Hive ransomware actor(s) because they are in the same hospital service market. The feared motivation for the selection of these targets was that during patient surges caused by the Covid-19 Delta Variant, a coordinated attack against medical facilities serving the same market would increase the likelihood that one or all of these targets pay the ransom.

The Pennsylvania Criminal Intelligence Center (PaCIC) receives this communication since they belong to CIN. After contacting the NY SIC, PaCIC publishes a Critical Infrastructure and key Resource (CIKR) Information Alert informing their public and private sector cybersecurity intelligence subscribers of this development.

**Inject 3 - <Insert Date and Time (1 Hour Before Start)>**

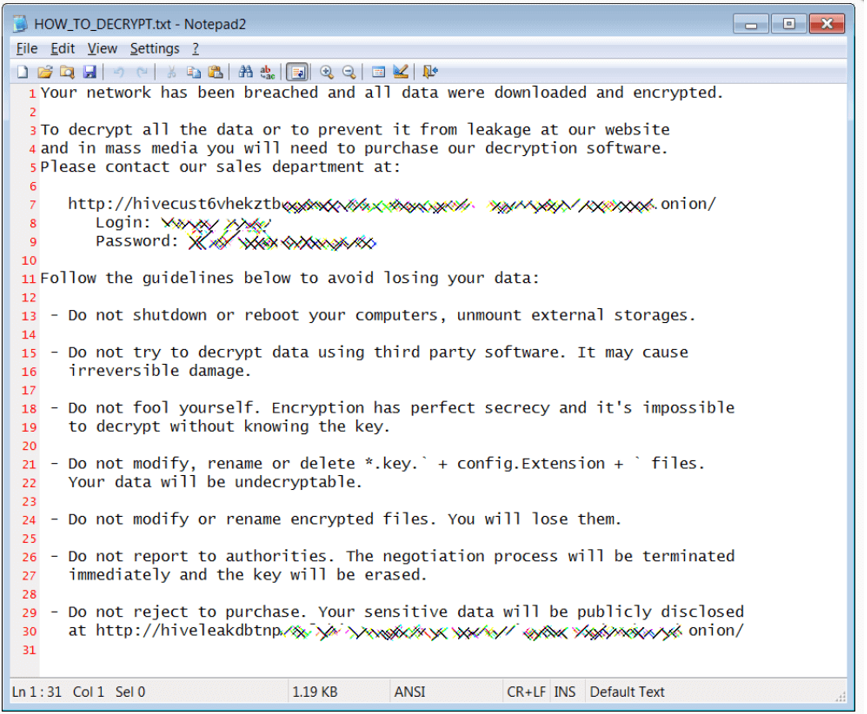
A clinical staff member of the emergency department of XXXX County Medical Center, a XXX-bed hospital and Level 1 trauma center in XXXX, PA reported a problem accessing patients records to their IT help desk.

Upon being notified of the problem, an IT technician remotely entered into the hospital’s Electronic Health Record (EHR) system and found the records encrypted with a “.hive” extension. A file named *HOW-TO-DECRYPT.txt* was added to all impacted directories.

The IT technician, who receives PaCIC cybersecurity products, recognized the threat. She notified the medical center’s Chief Information Officer (CIO). Following a pre-arranged script to prevent the additional spread of the ransomware, the CIO orders a shutdown of all IT systems, including the EHR system, emails and other hospital systems which support medical devices.

**Inject 3 - <Insert Date and Time (1 Hour Before Start, Continued)>**

Prior to the shutdown, the IT technician downloaded the *HOW-TO-DECRYPT.txt* file to a thumb drive and open the file on an offline laptop. The following message was revealed:



**Inject 4 - <Insert Date and Time (15 Minutes Before Start)>**

The CIO briefs the Hospital Administrator of the situation. The Hospital Administrator orders that the hospital be placed on ambulance divert to limit the number of patients coming into their emergency room. He orders the execution of existing contingency plans to mitigate the impact of the cyber incident which includes the use of paper-based patient charts and face-to-face communications.

**Inject 5 - <Insert Date and Time (Start)>**

XXXX County Medical Center contacts XXXX County 9-1-1 Center and reports the following information:

They have been a victim of a suspected ransomware attack, and they have lost access to their EHR system and other critical hospital systems.

They are declaring a Facility Emergency and need to institute an ambulance diversion. However, they are still accepting walk-in emergency room patients. Elective procedures are being cancelled until further notice.

With the manual processes and other contingencies being implemented, they are currently reporting no unmet needs.

**Inject 6 - <Insert Date and Time (Plus 15 Minutes)>**

Upon receiving notification of the call, a staff member of the XXXX County Emergency Management Agency contacts the XXXX County Medical Center to get additional information.

They are informed of the following:

This incident has already been reported to the local police, the FBI, the PaCIC, and the Pennsylvania Department of Health (DOH).

If the patient information in their EHR data base becomes public, they will have to start notifying impacted individuals.

The Medical Center has access to recently backed up copies of their EHR records and other digital backups through their cloud-based data recovery solution. Once they determine the full scope of attack, they will commence with reimaging their computer equipment, reloading software and switch over to uncompromised data.

Their hospital policy is to not negotiate with ransomware actors. They are confident that their data recovery solution will give them increasing functionality over the next couple of days and lead to a full recovery.

**Inject 7 - <Insert Date and Time (Plus 2 Hours) >**

An adjacent medical facility, Memorial Hospital, which has been accepting ambulances diverted from XXXX County Medical Center, contacts the XXXX County 9-1-1 Center to report the following:

They have suffered a suspected ransomware attack and lost the ability to access their EHRs other critical hospital systems.

Hospital staff is working to develop manual workarounds to overcome lost capabilities, but they find it necessary to initiate a hospital divert to ensure the safety of their existing patients. Patients are being contacted to cancel elective procedures.

They found a file named *HOW\_TO\_DECRYPT.txt* in their EHR database which confirmed their suspicions that their network has been breached, and data downloaded and encrypted.

Currently, they are not reporting any unmet needs and agree to keep XXXX County informed of their status.

**Inject 8 - <Insert Date and Time (2 Hours & 10 Minutes) >**

When informed of the second incident, the XXXX County Emergency Management Coordinator directs his staff to contact XXXX County Medical Center to get additional information. They are notified of the following:

This incident has been reported to DOH. They have contacted their cyber insurance provider which is assisting with remediation and recovery efforts.

Their cyber insurance provider has been in contact with the ransomware attacker. The attacker is demanding the equivalent of $144,000 in Bitcoins cryptocurrency in return for a key to unlock the hospital’s files and a promise to erase the patient records that were exfiltrated from their network.

The hospital has some digital data and software backups stored on physical mediums, but they not do not have recent backups of their EHRs. The hospital does not know how long it will take them to retrieve critical data or use of their systems.

A local news organization has already contacted the hospital about the incident. They are in the process of preparing a press release.

# Appendix A: Suggested Exercise Schedule

Please modify this suggested schedule to meet your needs.

| Date | November 2022 |
| --- | --- |
| 0900-1200 | |
| 0830-0900 | Registration |
| 0900-0915 | Welcome and Introductions |
| 0915-0945 | Module 1: Phishing |
| 0945-1030 | Module 2: Ransomware Attack |
| 1030-1045 | Break |
| 1045-1130 | Module 3: Containment, Eradication, Recovery |
| 1130-1200 | Hot Wash and Closing Comments |

# Appendix B: Acronyms

| **Acronym** | **Term** |
| --- | --- |
| AAR | After-Action Report |
| BOE | Board of Education |
| CISA | Cybersecurity and Infrastructure Security Agency |
| DDoS | Distributed Denial of Service |
| DHS | U.S. Department of Homeland Security |
| FBI | Federal Bureau of Investigation |
| HSEEP | Homeland Security Exercise and Evaluation Program |
| HVAC | Heating, Ventilation, and Air Conditioning |
| MS-ISAC | Multi-State Information Sharing & Analysis Center |
| IS | Information Systems |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| PII | Personally Identifiable Information |
| SitMan | Situation Manual |
| TTX | Tabletop Exercise |
| TLP | Traffic Light Protocol |

**Appendix C: Participant Feedback Form**

Please enter your responses in the form field or check box after the appropriate selection.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name:** |  | | | | | **Title:** |  |
| **Agency:** | |  | | |  |  |  |
| **Role:** | Player | | Facilitator | Observer | | Evaluator | |

**Part I: Recommendations and Corrective Actions**

1. Based on the discussions today and the tasks identified, list the top three strengths and/or areas that need improvement.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

1. Identify the action steps that should be taken to address the issues identified above. For each action step, indicate if it is a high, medium, or low priority.

| **Corrective Action** | **Priority** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. Describe the corrective actions that relate to your area of responsibility. Who should be assigned responsibility for each corrective action?

| **Corrective Action** | **Recommended Assignment** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. List the policies, plans, and procedures that should be reviewed, revised, or developed. Indicate the priority level for each.

| **Item for Review** | **Priority** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Part II: Participant Feedback**

What changes would you make to this exercise? Please provide any recommendations on how this exercise or future exercises could be improved or enhanced.

|  |
| --- |
|  |
|  |
|  |
|  |
|  |