<Enter Organization Name>

CISA Tabletop Exercise Package – Healthcare and Public Health Sector

<Exercise Date>

Table of Contents

Handling Instructions

Delete instructions that are not applicable.

The Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries that are applied to the recipient(s) of the information.[1] Select one of the following TLP designations below for this CISA Tabletop Exercise Package based on your information sharing needs.

TLP: WHITE

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as "*Traffic Light Protocol (TLP):WHITE*": Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. **Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.**

This document may be disseminated publicly pursuant to TLP:WHITE and <exercise sponsor name or other authority> guidelines.

For questions about this event or recommendations for improvement contact: <Name>, <Title> at <###-###-####> or <email address> of <sponsoring organization>.

TLP: GREEN

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as "*Traffic Light Protocol (TLP):GREEN*": Limited disclosure, restricted to the community. Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP:GREEN information may not be released outside of the community.**

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:GREEN and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: <Name>, <Title> at <###-###-####> or <email address> of <sponsoring organization>.

TLP: AMBER

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as "*Traffic Light Protocol (TLP):AMBER*": Limited disclosure, restricted to participants' organizations. This designation is used when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their

[1] CISA Traffic Light Protocol (TLP) definitions and usage. Retrieved 8 December 2021 from https://www.cisa.gov/tlp.

own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.**

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: <Name>, <Title> at <###-###-####> or <email address> of <sponsoring organization>.

TLP: RED

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as "*Traffic Light Protocol (TLP):RED*": Not for disclosure, restricted to participants only.

Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, **TLP:RED should be exchanged verbally or in-person**.

This document should be disseminated to applicable partners and stakeholders on a strict need-to-know basis pursuant to TLP:RED and <exercise sponsor name or other authority> guidelines due to the extreme sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: <Name>, <Title> at <###-###-####> or <email address> of <sponsoring organization>.

Exercise Overview

Exercise Name	Exercise Name	
Exercise Date, Time, and Location	Exercise Date Time (e.g., 9:00 a.m. – 12:00 p.m.) Exercise Location	
Exercise Schedule	**Time**	**Activity**
	Time	Activity
	Time	Activity
	Time	Activity
	Time	Activity
Scope	X hour facilitated, discussion-based Tabletop Exercise	
Purpose	Examine the coordination, collaboration, information sharing, and response capabilities of <Organization> in response to a cyber incident.	
NIST Framework Functions	For example, areas such as Identify, Protect, Respond, etc.	
Objectives	1. Examine the ability of <Organization> to respond to and recover from a significant cyber incident. 2. Discuss the impacts of a cyber incident on patient care and operations. 3. Assess <Organization>'s cybersecurity training program. 4. Explore <Organization>'s processes for information sharing, communications, and business continuity during a cyber incident. 5. Analyze <Organization>'s third-party vendor and patch management programs.	
Threat or Hazard	Cyber Threats	
Scenario	A threat actor targets <Organization> employees through phishing emails. Imaging equipment, patient records, and other hospital equipment begin malfunctioning/displaying incorrect data. <Organization> operations are reduced, PHI data is exfiltrated, and ransomware compromises computer systems and equipment, followed by social media backlash and media inquiries.	
Sponsor	Exercise Sponsor	
Participating Organizations	Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.)	
Points of Contact	**Insert Organization POC(s)** Contact info	**CISA Exercises** CEP@hq.dhs.gov

General Information

Exercise Guidelines

- This exercise will be held in an open, no-fault environment. Varying viewpoints are expected.
- Respond to the scenario using your knowledge of existing plans and capabilities, and insights derived from your training and experience.
- 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 and/or suggested actions to resolve or mitigate a problem.
- There is no hidden agenda, and there are no trick questions. The resources and written materials provided are the basis for discussion.
- The scenario has been developed in collaboration with subject matter experts and exercise planners from your organization.
- In any exercise, assumptions and artificialities are necessary to complete play in the time allotted, to achieve training objectives, and/or account for logistical limitations. Please do not allow these considerations to negatively impact your participation in the exercise.

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** 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** 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** provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise.
- **Note-takers** are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

Exercise Structure

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

- Cyber threat briefing (if desired)
- Scenario modules:
  - **Module 1:** A cybersecurity alert for healthcare organizations, a suspicious 401(k) email, unusual network traffic, and an unannounced visit by a vendor.
  - **Module 2:** 401(k) vendor was compromised by a cyberattack, imaging equipment is malfunctioning, patient records are displaying incorrect data, infusion pumps are faulty, and patient families critique the hospital online.

- **Module 3:** A ransomware message locks organization equipment, patients are solicited with their stolen data, local news stations ask for comment, patients request transfers to other hospitals along with their records.

- ***Structure Note:*** *Injects and discussion questions included in each module may be modified as desired, including involving those outside the Healthcare and Public Health sector. This exercise has been designed to explore several different threats to your organization, indicated in bold parentheses before the inject text. Your organization may select specific types of events and threats for your exercise and should delete any extra injects and discussion questions not relevant to your selected scenario. Additional discussion questions can be found in Appendix A.*

Exercise Hotwash

The facilitator will lead a hotwash with participants at the end of the exercise. The hotwash is an opportunity for exercise participants to discuss the strengths and weaknesses of their organization's response to the events presented during the exercise to address any ideas or issues that emerge from the exercise discussion.

Module 1

Day 1

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) release a joint alert regarding a rise in cyberattacks targeting healthcare organizations. The alert describes the tactics, techniques, and procedures (TTPs) used by cyber criminals, including phishing emails, ransomware, remote hacking, distributed denial of service (DDoS) attacks, and data exfiltration from healthcare organizations.

Day 9

Many employees receive an email from your company's 401(k) manager advising them of pending account changes and instructing recipients to click the link for more details. Employees that click on the link are taken to the website and are required to enter their credentials for access

Some employees contact <Human Resources (HR)/Benefits> asking why the changes have been made. <HR/Benefits> is unaware of any changes to the 401(k) and requests a copy of the email.

Day 10

During a routine review, the Information Technology (IT) Department discovers the network logs show an abnormally high volume of traffic during non-business hours. It is determined most of this traffic is outbound and being sent to unknown Internet Protocol (IP) addresses.

Day 21

A third-party electronic medical record (EMR) vendor shows up unannounced at your facility to update equipment. The vendor needs to patch a recently discovered vulnerability in software used on several devices, including workstations, imaging and radiology equipment, bedside monitors, and other clinical devices.

Discussion Questions

Your organization may select specific types of events and threats for your exercise and should delete any discussion questions not relevant to your selected scenario. Additional discussion questions for each module can be found in Appendix A.

1. What is the greatest cybersecurity risk to <Organization>?
2. What cyber threat information and intelligence do you receive?
    a. How do you collect and share this information?
    b. Who is responsible for collecting and disseminating this information?
    c. What information is most actionable?
3. What cybersecurity training does <Organization> provide its staff?
    a. How often must they complete this training?
    b. What happens if training is not completed?
    c. Who is required to complete this training?
4. How do users report suspicious emails?
    a. What procedures or plans would be followed once a suspicious email has been reported?
5. Describe your patching and security protocols for third-party technology vendors.
    a. How do vendors notify you that maintenance and updates are required?
    b. What security concerns do you have about your third-party vendors?

   c. What cyber training do you require your vendors to complete?
6. How would you describe <Organization>'s cybersecurity posture?
   a. What types of Multi-Factor Authentication (MFA) does your organization use?
   b. How frequently are users required to change their passwords?
   c. How does <Organization> mitigate the potential effects of phishing?

Module 2

Day 35

Your 401(k) management vendor notifies you that they were recently the target of a malware attack that compromised their business email. They confirm the email your employees received came from their system but was not sent by them. They also confirm that the site accessed through the link in the spoofed email was not legitimate.

Day 47 – Morning

Technicians begin reporting the imaging equipment is not performing properly. They report blurred images, incorrectly formatted images, and images containing incorrect patient data.

Day 47 – Mid-Morning

Nurses on the floor report that patient records are displaying incorrect information about medication, diagnosis, and personal information.

Day 47 – Afternoon

Staff discover bedside monitor data is inaccurate and the infusion pumps are not operating properly and are failing to deliver infusions at the correct rate.

Day 49

Several patients' families overhear hospital staff talking about the problems with medical records and infusion pumps and demand to know if the issues are affecting their family members. They begin posting on social media about the issues the hospital is experiencing and wondering just how safe it is to be there.

Discussion Questions

Your organization may select specific types of events and threats for your exercise and should delete any discussion questions not relevant to your selected scenario. Additional discussion questions for each module can be found in Appendix A.

1. What are your priorities?
2. How would you rate the severity of these events?
    a. Would this activate your response team?
        i. How is this determined?
3. Describe the role cybersecurity has in your third-party vendor contracts.
    a. Are your vendors contractually required to notify you of cyber incidents?
    b. How well do <Organization> service level agreements address incident response?
4. How are your EMR and business data backed up?
5. Describe your manual procedures. At what point would they be initiated?
    a. How long can you effectively operate on manual procedures?
    b. How long will it take to enter paper-based data into the EMR once manual procedures end?
6. How do you respond to social media posts about these events?
    a. What does your organization do to monitor social media?
    b. What is your social media policy for employees?

Module 3

Day 58

Hospital staff start experiencing issues with their computers freezing, and work devices begin shutting down. When devices restart, employees are locked out of their machines and their screens display a ransomware message that reads:

> "Hello! Your files have been encrypted, but do not fear because for the sum of $<XXXX> in cryptocurrency, your files will be returned. The decryption key will expire in 72 hours. Please submit payment to the wallet below or you will not be able to recover your files."

Day 60

Current and former patients contact the hospital saying they have been called by people claiming to have access to their medical records and offering to return them for a fee. The patients are given enough information to verify the callers have their records.

Patients say the fees range from a few hundred dollars to more than a thousand and are demanding to know how these individuals could have their records.

Some say they have contacted law enforcement; others have contacted the media. Many are threatening to sue. Others are posting about the incident on social media.

Day 61

Local news stations contact the hospital for comment and some stations arrive at the hospital to begin live broadcasts for the evening news.

Day 63

Patients begin requesting transfers to other local hospitals, as they feel unsafe. They also demand the return of all their medical records, as well as the removal of them from your network. They state that neither they nor their families will be treated in your facilities again.

Discussion Questions

Your organization may select specific types of events and threats for your exercise and should delete any discussion questions not relevant to your selected scenario. Additional discussion questions for each module can be found in Appendix A.

1. How have your priorities changed based on the events of Module 3?
2. What actions would be taken based on your incident response plan?
    a. What ransomware policies and procedures are included in your incident response plan?
    b. What does your cyber insurance policy cover?
3. What is the decision-making process for ransomware payment?
    a. How are your cyber insurance providers involved in your procedures?
    b. What are the advantages/disadvantages to agreeing/refusing to pay?
    c. What are the potential legal and reputation ramifications?
4. What is your threshold for contacting law enforcement during a cyber incident?
5. What concerns would arise with the discovery of protected health information (PHI) of patients being available to unauthorized personnel?
    a. Does the loss of PHI affect your decision to pay the ransom?

6. Do you have a communications plan that addresses cyber incidents?
    a. How will you ensure accuracy and timeliness of information being shared with staff, patients, and families?
    b. How would <Organization> address these incidents with the local media?
    c. How would <Organization> respond to the social media posts and patient complaints?
7. What are your concerns with regards to these events impacting <Organization> reputation in the community?

Appendix A: Additional Discussion Questions

The following section includes supplemental discussion questions to guide exercise play. Questions are aligned to the NIST functional areas, specific attack vectors, and roles. Exercise planners are encouraged to select additional, applicable discussion questions to the chosen scenario to bolster participant conversation.

This instructional page, as well as undesired discussion questions, should be deleted.

Cyber Preparedness and Planning

1. How does <Organization>'s incident response plan aid in the mitigation of the cyberattacks presented?
2. How does <Organization> integrate cybersecurity into the system development life cycle (i.e., design, procurement, installation, operation, and disposal)?
3. What level of funding and/or resources are devoted to cyber preparedness? Based on your risk assessment, what is the range of potential losses from a cyber incident?
4. What mission essential functions depend on information technology and what are the cascading effects of their disruption?
5. What external reviews or audits of your IT plans, policies, or procedures have been conducted within the last year?
6. Who oversees cybersecurity management?
7. What role does organizational leadership play in cybersecurity?
8. How do you communicate your cybersecurity concerns to your vendors and how do you evaluate their cybersecurity performance?
9. How well-defined is cybersecurity in relation to contracts with third-party support vendors and crucial suppliers?
    a. How often are contracts reviewed?
    b. How well do <Organization> service level agreements address incident response?
10. How does <Organization> baseline network activity?
    a. How would <Organization> be able to distinguish between normal and abnormal traffic?
11. What type of hardware and/or software does <Organization> use to detect/prevent malicious activity of unknown origin on <Organization> systems/network?
12. What is the procedure for deploying high priority patches of user applications and software?
13. How are employees trained to recognize and report cyber threats such as phishing scams?
    a. What additional training does <Organization> require for those who fall for a fake phishing campaign?
14. What multi-factor authentication methods (e.g., something you know, something you have, something you are) does <Organization> utilize to mitigate the potential effects of phishing?
15. What is the password management policy for <Organization> local or internal network?
16. How regularly are users required to change their passwords?
    a. What is <Organization> account lockout policy if users don't change their passwords in a timely fashion?
    b. What are <Organization> requirements for password length and level of complexity?

Information Sharing

1. What established mechanisms does <Organization> have to facilitate rapid information dissemination?
    a. What are <Organization>'s known communication gaps? Who in <Organization> is responsible for addressing those gaps?
2. What other sources of cybersecurity threat intelligence does <Organization> receive (e.g., information from FBI, H-ISAC, HHS, open-source reporting, security service providers)?
    a. What cyber threat information is most useful, timely, and actionable?
    b. Who is responsible for collating/disseminating information across <Organization>?
3. What mechanisms and products are used to share cyber threat information within <Organization> and externally (e.g., distribution lists, information sharing portals)?
4. Describe how variables in threat information (timeframe, credibility, and specificity) impact decision making.
5. What are some challenges that are experienced by information technology and business continuity planning in terms of information sharing? Is information flowing in both directions?

Incident Response

1. When was <Organization>'s cybersecurity incident response plan issued and when was the plan last revised?
2. What key contact information is included in <Organization>'s incident response plan if you suspect you have experienced a cyber incident?
3. When do <Organization> IT and helpdesk staff conduct network maintenance (e.g., specific days or times of day)?
4. How would these events affect your organization's business operation/processes?
5. What is <Organization> IT department's patch management plan?
    a. What risk assessments are performed on all servers on the network?
    b. What processes exist to evaluate each server's criticality and applicability to software patches?
6. What resources and capabilities are available to analyze an intrusion or mitigate the incident?
    a. Internally?
    b. Through the private sector (third-party vendors)?
    c. Through government partners?
7. Describe the decision-making process for protective actions in a cyber incident.
    a. What options are available?
    b. What options are documented in plans?
    c. How are they activated?
8. What immediate protection and mitigation actions would be taken at <Organization> in this scenario? Who is responsible for those actions?
9. How would your organization respond to the discovery of a malicious, unauthorized administrator account on your systems? Who would be informed internally? Who would be informed externally (e.g., law enforcement, cybersecurity insurance partners, etc.)?
10. What detection methods does <Organization> have to identify a compromise?
11. What protective actions would <Organization> take across non-impacted systems in the scenario presented?
    a. Who is responsible for protective action decision-making?

   b. How are actions coordinated across parts of <Organization>?
12. How would you rate this security incident severity for <Organization>? What additional notifications or actions would this prompt?
13. What mission essential functions are impacted by the incidents described in the scenario?
14. Describe whether this scenario exceeds <Organization>'s ability to respond.
   a. If so, what are the established procedures to request additional support?
15. Who does <Organization> receive cyber response technical assistance from?
   a. What plans and procedures exist to access this assistance?
16. What service provider relationships are needed for incident/breach response issues (e.g., credit counseling, forensic/computer security services)?
   a. What are some challenges that are experienced by information technology and business continuity planning in terms of information sharing? Is information flowing in both directions?
17. What processes are used to contact critical personnel at any time, especially outside of business hours?
   a. How does <Organization> proceed if critical personnel are unreachable or unavailable?
18. What alternative systems or manual processes are available to continue operations if a critical system is unavailable for a significant period?
   a. Who can authorize use of alternate systems or procedures?
19. When and how does <Organization> determine a cyber incident is closed?
20. What are <Organization>'s defined cybersecurity incident escalation criteria, notifications, activations, and/or courses of action?
   a. Where does this incident fall within the incident severity schema for <Organization>?
   b. When would leadership be notified?
21. When would <Organization>'s cyber incident response team be activated?
   a. What are their priorities?
22. What incident de-escalation procedures are in place?
   a. What quantifiable, repeatable process exist for determining when an incident is resolved and when the incident response team can stand down?
23. Describe <Organization>'s After-Action Report or lessons learned process.
   a. Who leads this process for a cyber incident?
   b. How are recommended improvements implemented and tested?
24. What remediation is required of employees to ensure an event like this does not happen again (training, self-education, etc.)?

Ransomware

1. What resources are required for incident investigation and attribution?
2. If you were one of the individuals who received the ransom demand, who would you inform, internally? Who would you inform externally?
3. How is ransomware addressed in <Organization>'s incident response plan?
   a. How frequently does <Organization> exercise your response to ransomware?
4. What formal policies and procedures does <Organization> have to document the process for restoring backed-up data?
   a. How does <Organization> ensure the integrity of backed-up data before restoration?

5. Where does <Organization> store back-ups of vital records? Are your backups stored in a location that is separated from your primary working copies of your files?
    a. How long does <Organization> keep any copies of archived files backed up?
    b. How long of a downtime would exist between loss of your primary files and the restoration of files via your back-up?
6. What processes and resources are used for evidence preservation and forensics?
    a. When would <Organization> engage law enforcement, if at all?
    b. Who would <Organization> be contacting from local, state, and federal entities?
7. What steps would be taken to regain access to locked accounts?
    a. What training do employees receive for this situation?

Training and Exercises

1. How do employees report suspected phishing attempts?
    a. What actions does <Organization> take when suspicious emails are reported?
    b. What formal policies or plans would be followed?
    c. What training do employees receive on phishing (e.g., phishing self-assessments)?
2. What basic cybersecurity and/or IT security awareness training does your organization provide to all users (including managers and senior executives)?
    a. How often is training provided?
    b. What topics are covered in your training?
    c. What training is required to obtain network access?
    d. What security-related training does your department or agency provide to, or contractually require of, IT personnel and vendors with access to your organization's information systems? How often do they receive the training?
3. What special training, if any, do your cybersecurity incident response team members undergo to detect, analyze, and report this activity? Describe this training.
    a. How is your staff trained to read and analyze your intrusion detection system logs?
4. What are your cybersecurity incident response team's exercise requirements?
5. How does your organization's efforts address both physical and cyber risks?
6. Describe the level of involvement and participation of senior or elected officials in your cybersecurity exercises.
7. What are the additional training and/or exercising requirements for your organization?

Data Exfiltration

1. What actions would be taken when the exfiltration is discovered? Does <Organization> have written plans that would be implemented?
2. What impact will the potential sale of patient' sensitive or PHI have on <Organization> response and recovery activities?
    a. What is IT's reporting process?
    b. How have <Organization> public relations priorities changed?
    c. What additional legal or regulatory notifications are required?

Public Affairs

1. What steps would be taken to address the public following these cyber incidents?

   a. How would patients be notified about the cyberattacks?
2. Who is responsible for public information dissemination related to the incident? What training or preparation have they received?
3. Who would the public relations team contact in the event of an incident? How are these contacts prioritized?
4. What online resources and communication formats does <Organization> use to keep patients, families, and the public informed regarding any incidents?
5. How would your organization respond to the emerging news and social media issues?
   a. What communications processes would be used for immediate release of messages? Does your organization have pre-approved messages?

Legal

1. What are the legal issues <Organization> must address?
2. What legal documents should your organization have (e.g., with third-party vendors)?
3. What is the role of the legal department in this scenario?
4. What are <Organization>'s security breach notification laws? What do they include?
5. What security breach notification laws does your state have? What do these laws include?
6. What processes exist to collect evidence and maintain the chain of custody?

Appendix B: Acronyms

Acronym	Definition
CISA	Cybersecurity and Infrastructure Security Agency
DDoS	Distributed Denial of Service
DHS	U.S. Department of Homeland Security
EMR	Electronic Medical Record
FBI	Federal Bureau of Investigation
HHS	U.S. Department of Health and Human Services
H-ISAC	Health Information Sharing and Analysis Center
HR	Human Resources
IP	Internet Protocol
IT	Information Technology
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
PHI	Protected Health Information
POC	Point of Contact
TLP	Traffic Light Protocol
TTP	Tactics, Techniques, and Procedures
UHS	Universal Health Services
UVM	University of Vermont

Appendix C: Case Studies

Ransomware

University of Vermont Medical Center Ransomware

On October 28, 2020, the University of Vermont (UVM) Medical Center information technology (IT) desk received dozens of calls from staff complaining of computer access problems. When staff began investigating for malicious software, they found a file with instructions to contact the alleged perpetrators of the cyberattack. To prevent further damage, the UVM Center locked down email, internet access, and major chunks of the organization's computer network.

As a result of the shutdown, UVM Medical Center employees couldn't use electronic health records, payroll programs, and other vital digital tools nearly a month. For days, staff didn't even know which patients were scheduled for appointments. Urgent surgeries were rescheduled, and cancer patients had to go elsewhere for radiation treatment.

The Center did not pay the ransom, but the attack still cost an estimated $50 million, mostly from lost revenue, says UVM Health Network Chief Medical Information Officer Doug Gentile, MD. It took IT staff three weeks of working 24/7 to scrub network systems and restore capability to the thousands of affected computers.[2]

Universal Health Services Ransomware

Universal Health Services (UHS) operates 400 hospitals and behavioral health facilities in the United States and United Kingdom and, in September 2020, a cyberattack wiped out all its IT systems.

Phone systems were no longer functioning and, without access to computers and electronic health records, employees had to resort to pen and paper to record patient information. Initially, the health system was forced to divert ambulances to alternative facilities and some elective procedures were either postponed or transferred elsewhere. Patients also reported delays receiving test results while UHS recovered from the attack.

While UHS worked quickly to restore its information technology infrastructure, the recovery process still took nearly three weeks. Naturally, this disruption also entailed a major financial impact: the UHS quarterly earnings report for Q4 2020 showed approximately $42.1 million in losses. Restoring the IT infrastructure resulted in a significant increase in labor costs, both internally and externally, and UHS reported total pre-tax losses of an estimated $67 million due to the ransomware attack.[3]

Springhill Medical Center Ransomware Death

In July 2019, the Springhill Medical Center suffered a ransomware attack and was forced to operate without the full function of its computer systems for nearly eight days. Patient records were inaccessible and medical staff were unable to use equipment to monitor fetal heartbeats.

---

[2] Weiner, Stacy (2021, July 20). *The growing threat of ransomware attacks on hospitals.* Retrieved from the Association of American Medical Colleges (AAMC): The growing threat of ransomware attacks on hospitals | AAMC

[3] Alder, Steve (2021, March 1). *Universal Health Services Ransomware Attack Cost $67 Million in 2020.* Retrieved from HIPAA Journal: Universal Health Services Ransomware Attack Cost $67 Million in 2020 (hipaajournal.com)

While these systems were down, a baby was born at the hospital with her umbilical cord wrapped around her neck. The child suffered severe brain damage as a result of the delivery, and she died nine months later due to related complications. Katelyn Parnell, MD, attending OB-GYN at the hospital, texted the nurse manager that she would have delivered the baby by cesarean had she seen the monitor readout.[4] The fetal heartbeat monitor would have indicated the distress caused by the umbilical cord, and provided information so emergency intervention could be performed. Now, the mother is suing the hospital and, if the lawsuit is successful, this will be the first case of a death due to a ransomware attack in the United States.[5]

Malware and Data Theft

Florida Orthopedic Institute Data Breach

The Florida Orthopedic Institute's servers were infiltrated by malicious actors who then encrypted patients' files, blocking access to them by the facility's staff members on April 9, 2020. According to the HHS Office for Civil Rights breach portal, the attackers gained access to the PHI of approximately 640,000 individuals.[6] The Florida Orthopedic Institute's own investigation also uncovered reasons to suspect that some of the patients' complete identities had been stolen before the encryption, which would include data points such as names, birthdates, Social Security numbers, and more.

While the Florida Orthopedic Institute has not found evidence that those identities have been used, the Institute is facing a class-action lawsuit due to the data breach. Current and former patients are seeking at least $99 million, citing a "failure to properly secure and safeguard protected health information," according to the complaint filed June 30, 2020.[7]

Twelve Oaks Recovery Malware and Data Breach

On December 13, 2020, Twelve Oaks Recovery, a Florida-based addiction and mental health treatment center, detected unusual network activity. Upon further investigation, they discovered that an unauthorized individual had gained access to its network, installed malware, and stole documents from its systems. A forensic investigation confirmed that malware had been deployed on December 13, 2020 and data exfiltration was confirmed the following day.

The attacker obtained documents that contained the PHI of 9,023 patients, including names, addresses, dates of birth, medical record numbers, and Social Security numbers.[8]

[4] U.S. Department of Health and Human Services (2022, March 03). *Heath Sector Cybersecurity: 2021 Retrospective and 2022 Look Ahead*. Retrieved from: Department of Health and Human Services

[5] Mitchell, Hannah (2021, September 30). Cyberattack on Alabama hospital linked to 1st alleged ransomware death. Retrieved from: Cyberattack on Alabama hospital linked to 1st alleged ransomware death (beckershospitalreview.com)

[6] U.S. Department of Health and Human Services Office for Civil Rights. *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*. Retrieved from: U.S. Department of Health & Human Services - Office for Civil Rights (hhs.gov)

[7] Calaway, Jackie (2020, July 2*). One of Florida's largest orthopedic providers faces class-action lawsuit after data breach.* Retrieved from ABC News: Fla. orthopedic provider faces class-action lawsuit after data breach (abcactionnews.com)

[8] Alder, Steve (2021, March 2). *Roundup of Recent Healthcare Phishing and Malware Incidents.* Retrieved from HIPAA Journal: Roundup of Recent Healthcare Phishing and Malware Incidents (hipaajournal.com)

Phishing

Utah Pathology Services

One June 30, 2020, Utah Pathology Services discovered that hackers had gained access to their systems via an employee's compromised email account. Using the compromised account, the hackers tried to redirect funds from the organization but were ultimately unsuccessful.

The hack prompted an investigation, which revealed that multiple employees were the victims of an email phishing scheme. Further, approximately 148,594 individuals may have had their PHI exposed. The PHI involved included names, dates of birth, gender, telephone numbers, addresses, health insurance information, clinical and diagnostic information, and Social Security numbers.[9]

[9] U.S. Department of Health and Human Services Office for Civil Rights. *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*. Retrieved from: U.S. Department of Health & Human Services - Office for Civil Rights (hhs.gov)

Appendix D: Attacks and Facts

Distributed Denial of Service

Distributed Denial of Service (DDoS) attacks overload bandwidth and connection limits of hosts or networking equipment, specifically through a network of computers making excessive connection requests. DDoS attacks unfold in stages. First, a malicious actor infects a computer with malware that spreads across a network. This infected computer is known as the "master" because it controls any subsequent computers that become infected. The other infected computers carry out the actual attack and are known as "daemons." The attack begins when the master computer sends a command to the daemons, which includes the address of the target. Large numbers of data packets are sent to this address, where extremely high volumes (floods) of data slow down web server performance and prevent acceptance of legitimate network traffic. The cost of a DDoS attack can pose sever loss of revenue or reputation to the victim.

More information on DDoS attack possibilities within each layer of the OSI Model, as well as traffic types and mitigation strategies, can be found in the resource list below.

Additional Resources

- Understanding Denial-of-Service Attacks (https://www.cisa.gov/uscert/ncas/tips/ST04-015)
- DDoS Quick Guide (https://www.cisa.gov/uscert/sites/default/files/publications/DDoS%20Quick%20Guide.pdf)
- Guide to DDoS Attacks (https://www.cisecurity.org/wp-content/uploads/2017/03/Guide-to-DDoS-Attacks-November-2017.pdf)

Social Engineering and Phishing

One of the most prominent tactics attackers use to exploit network and system vulnerabilities is social engineering–the manipulation of users through human interaction and the formation of trust and confidence to compromise proprietary information. Techniques for uncovering this information largely involve the use of phishing, i.e., email or malicious websites that solicit personal information by posing as a trustworthy source. Social engineering is effective for breaching networks, evading intrusion detection systems without leaving a log trail, and is completely dependent on the operating system platform. While technical exploits aim to bypass security software, social engineering exploits are more difficult to guard against due to the human factor. Organizations should take steps towards strengthening employee cybersecurity awareness training, to include training personnel to be cautious of suspicious emails, know where to forward them and keeping software and systems up to date.

Additional Resources

- Avoiding Social Engineering and Phishing Attacks (https://www.cisa.gov/uscert/ncas/tips/ST04-014)
- The Most Common Social Engineering Attacks (https://resources.infosecinstitute.com/common-social-engineering-attacks/)

Ransomware

Ransomware is a type of malware that denies access to victims' data or systems through encryption with a key only known by the malicious actor who deployed the malware. Once encrypted, the ransomware directs the victim to pay the attacker, typically in the form of cryptocurrency, so the victim can receive a decryption key. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. Recovery can be an arduous process and there is no guarantee the victim will receive access to their data or systems if the ransom is paid. For more information on best practices to protect users from the threat of ransomware, as well as recent Alerts on specific ransomware threats, see the resource list below.

Additional Resources

- CISA Stop Ransomware Website (https://stopransomware.gov)
- Protecting Against Ransomware (https://www.cisa.gov/uscert/ncas/tips/ST19-001)
- Indicators Associated With WannaCry Ransomware (https://www.cisa.gov/uscert/ncas/alerts/TA17-132A)
- Incident trends report (Ransomware) (https://www.ncsc.gov.uk/report/incident-trends-report#ransomware)

Appendix E: Doctrine and Resources

Laws

- National Cybersecurity Protection Act of 2014 (Dec 2014) (https://www.congress.gov/bill/113th-congress/senate-bill/2519)
- Federal Information Security Modernization Act of 2014 (Dec 2014) (https://www.cisa.gov/federal-information-security-modernization-act)
- Office of Management and Budget (OMB) Memorandum: M-15-01, Fiscal Year 2014-2015: Guidance on Improving Federal Information Security and Privacy Management Practices (Oct 2014) (https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf)

Presidential Directives

- Executive Order 14028: Improving the Nation's Cybersecurity (May 2021) (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)
- Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017) (https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/)
- Presidential Policy Directive 41: United States Cyber Incident Coordination (Jul 2016) (https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident)
- Annex to Presidential Policy Directive 41: Annex to the Directive on United States Cyber Incident Coordination (Jul 2016) (https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident)
- Presidential Policy Directive 8: National Preparedness (Mar 2011, Updated Sep 2015) (https://www.dhs.gov/presidential-policy-directive-8-national-preparedness)
- Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (Feb 2013) (https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)
- Executive Order 13636: Improving Critical Infrastructure Cybersecurity (Feb 2013) (https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity)

Strategies and Frameworks

- New Federal Government Cybersecurity Incident and Vulnerability Response Playbooks (Nov 2021) (https://www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability)
- National Cyber Strategy of the United States of America (Sep 2018) (https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf)
- U.S. Department of Homeland Security Cybersecurity Strategy (May 2018) (https://www.dhs.gov/publication/dhs-cybersecurity-strategy)

- Framework for Improving Critical Infrastructure Cybersecurity (Apr 2018) (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf)
- National Cyber Incident Response Plan (NCIRP) (Dec 2016) (https://www.cisa.gov/uscert/ncirp)
- National Protection Framework, Second Edition (Jun 2016) (https://www.fema.gov/sites/default/files/2020-04/National_Protection_Framework2nd-june2016.pdf)
- OMB Memorandum: M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government (Oct 2015) (https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf)

Key Points of Contact

- DHS CISA (contact: central@cisa.dhs.gov)
- FBI
    - Field Office Cyber Task Forces (contact: https://www.fbi.gov/contact-us/field-offices)
    - Internet Crime Complain Center (IC3) (contact: http://www.ic3.gov)
    - National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: cywatch@ic.fbi.gov; 855-292-3937)
- Health Sector Cybersecurity Coordination Center (HC3) (HC3@hhs.gov)
    - HC3 Products (Health Sector Cybersecurity Coordination Center (HC3) | HHS.gov)
- The Division of Critical Infrastructure Protection (CIP), the Sector Risk Management Agency (SRMA) for the Department of Health and Human Services (cip@hhs.gov)
- United States Secret Service Field Offices and Electronic Crimes Task Force (ECTFs) (contact: https://www.secretservice.gov/contact/field-offices/, https://www.secretservice.gov/investigation/cyber)

Other Available Resources

- Health and Human Services 405(d) Aligning Health Care Industry Security Approaches (https://405d.hhs.gov/resources)
- Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: info@msisac.org; (518) 266-3460)
- Cybersecurity and the States (National Association of State Chief Information Officers [NASCIO]) (http://www.nascio.org/Advocacy/Cybersecurity)
- National Governors Association (NGA) (https://www.nga.org/)
    - NGA Center for Best Practices (https://www.nga.org/bestpractices/divisions/hsps/)
- DHS Cybersecurity Fusion Centers (https://www.dhs.gov/state-and-major-urban-area-fusion-centers)
- InfraGard (https://www.infragard.org/)
- Internet Security Alliance (http://www.isalliance.org/)
- Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) (https://www.isao.org/information-sharing-groups/)
    - International Association of Certified ISAOs (http://www.certifiedisao.org; contact: operations@certifiedisao.org)

- National Council of ISACs (https://www.nationalisacs.org/)

Works Cited

Alder, S. (2021, March 1). Universal Health Services Ransomware Attack Cost $67 Million in 2020 Retrieved 2022, from HIPAA Journal: https://www.hipaajournal.com/universal-health-services-ransomware-attack-cost-67-million-in-2020/

Alder, S. (2021, March 2). Roundup of Recent Healthcare Phishing and Malware Incidents. Retrieved from HIPAA Journal: https://www.hipaajournal.com/roundup-of-recent-healthcare-phishing-and-malware-incidents/

Calaway, J. (2020, July 2). One of Florida's largest orthopedic providers faces class-action lawsuit after data breach. Retrieved from ABC News : https://www.abcactionnews.com/money/consumer/taking-action-for-you/one-of-floridas-largest-orthopedic-providers-faces-class-action-lawsuit-after-data-breach

Mitchell, H. (2021, September 30). *Cyberattack on Alabama hospital linked to 1st alleged ransomware death*. Retrieved from https://www.beckershospitalreview.com/cybersecurity/cyberattack-on-alabama-hospital-linked-to-1st-alleged-ransomware-death.html

U.S. Department of Health and Human Services. (2022, March 3). *Health Sector Cybersecurity: 2021 Retrospective and 2022 Look Ahead*. Retrieved from https://www.hhs.gov/sites/default/files/2021-retrospective-and-2022-look-ahead-tlpwhite.pdf

U.S. Department of Health and Human Services Office for Civil Rights. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

U.S. Department of Health and Human Services Office for Civil Rights. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Weiner, S. (2021, July 20). *The growing threat of ransomware attack on hospitals*. Retrieved from Association of American Medical Colleges: https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals