CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

LOUISIANA HEALTHCARE CYBER TABLETOP EXERCISE

MAY 23, 2023

Exercise Facilitator

Kristin Lockwood

Cyber Exercise Analyst

Cybersecurity and Infrastructure Security Agency (CISA)

National Cyber Exercise Program (NCEP)

OPENING REMARKS

Opening Remarks

Nicole Coarsey

Division Manager, Healthcare Access

Well-Ahead Louisiana

WELL-AHEAD

WELLAHEADLA.COM

THREAT BRIEFING

Threat Briefing

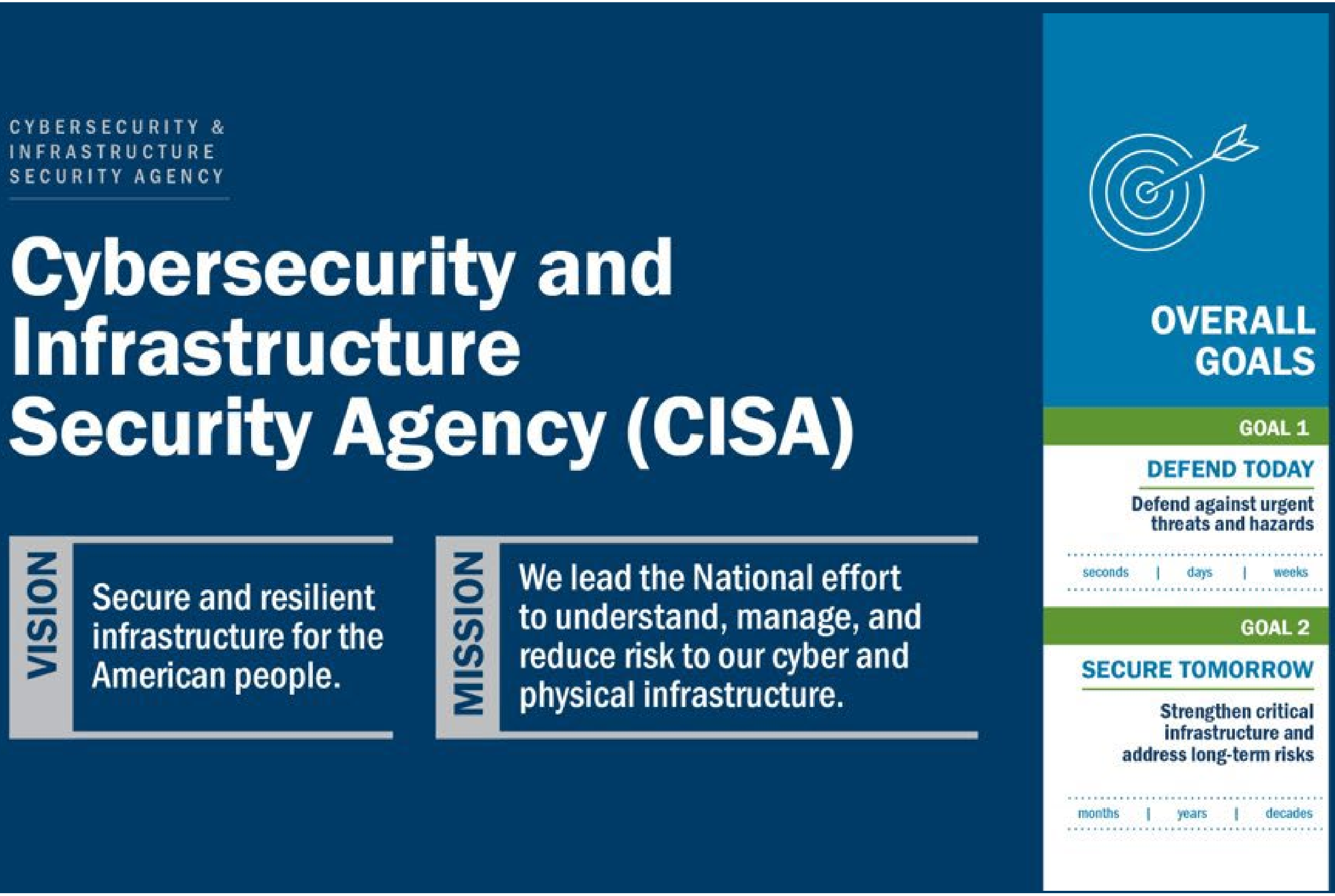
Nasreen Poptani

Cyber Threat Intelligence Analyst

Multi-State Information Sharing and Analysis Center

MS-ISAC®

Multi-State Information Sharing & Analysis Center®



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

months | years | decades

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Our Work

The Cybersecurity and Infrastructure Security Agency (CISA) works with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future

- PARTNERSHIP DEVELOPMENT
- INFORMATION AND DATA SHARING
- CAPACITY BUILDING
- INCIDENT MANAGEMENT & RESPONSE
- RISK ASSESSMENT AND ANALYSIS
- NETWORK DEFENSE
- EMERGENCY COMMUNICATIONS

Housekeeping Information

- Please remain on mute unless you are speaking
- Please download exercise materials:
  - Situation Manual
  - Slide Presentation

Security Protocol

- **Traffic Light Protocol (TLP): TLP:CLEAR**
  - Recipients can spread this to the world, there is no limit on disclosure.
  - Sources may use **TLP:CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.
- For reference purposes and additional information on TLP: https://www.cisa.gov/tlp

Exercise Schedule

Time (CDT)	Duration	Activity
1:00 p.m. – 1:05 p.m.	5 min	Welcome and Opening Remarks
1:05 p.m. – 1:20 p.m.	15 min	Threat Briefing
1:20 p.m. – 1:25 p.m.	5 min	Exercise Overview
1:25 p.m. – 2:05 p.m.	40 min	Module 1
2:05 p.m. – 2:10 p.m.	5 min	Break
2:10 p.m. – 2:55 p.m.	45 min	Module 2
2:55 p.m. – 3:05 p.m.	10 min	Break
3:05 p.m. – 3:50 p.m.	45 min	Module 3
3:50 p.m. – 4:00 p.m.	10 min	Hotwash and Closing Comments

Exercise Guidelines

- Open, no-fault, low-stress discussion
- Scenario
  - Developed with help from your experts
  - Only a snapshot
  - Focus on how you would respond if this happened, and not whether this could happen
- Post-Exercise
  - Draft Summary Report: Approximately TTX + 10 business days
  - Follow-up Survey from the Office of Personnel Management (OPM) approximately 6 months after the exercise

Participant Feedback Form

- Provide immediate feedback on the exercise
- You can start it now and finish it after the exercise
- Data from the form is included in the Summary Report and is used to improve future exercise offerings
- Scan the QR code:

Exercise Purpose

Examine the coordination, collaboration, information sharing, and response capabilities of rural healthcare facilities in response to a cyber incident.

Exercise Objectives

1. Examine the ability of rural healthcare facilities 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 rural healthcare facilities' cybersecurity training program.
4. Explore rural healthcare facilities' processes for information sharing, communications, and business continuity during a cyber incident.
5. Analyze rural healthcare facilities' third-party vendor and patch management programs.

Roles and Responsibilities

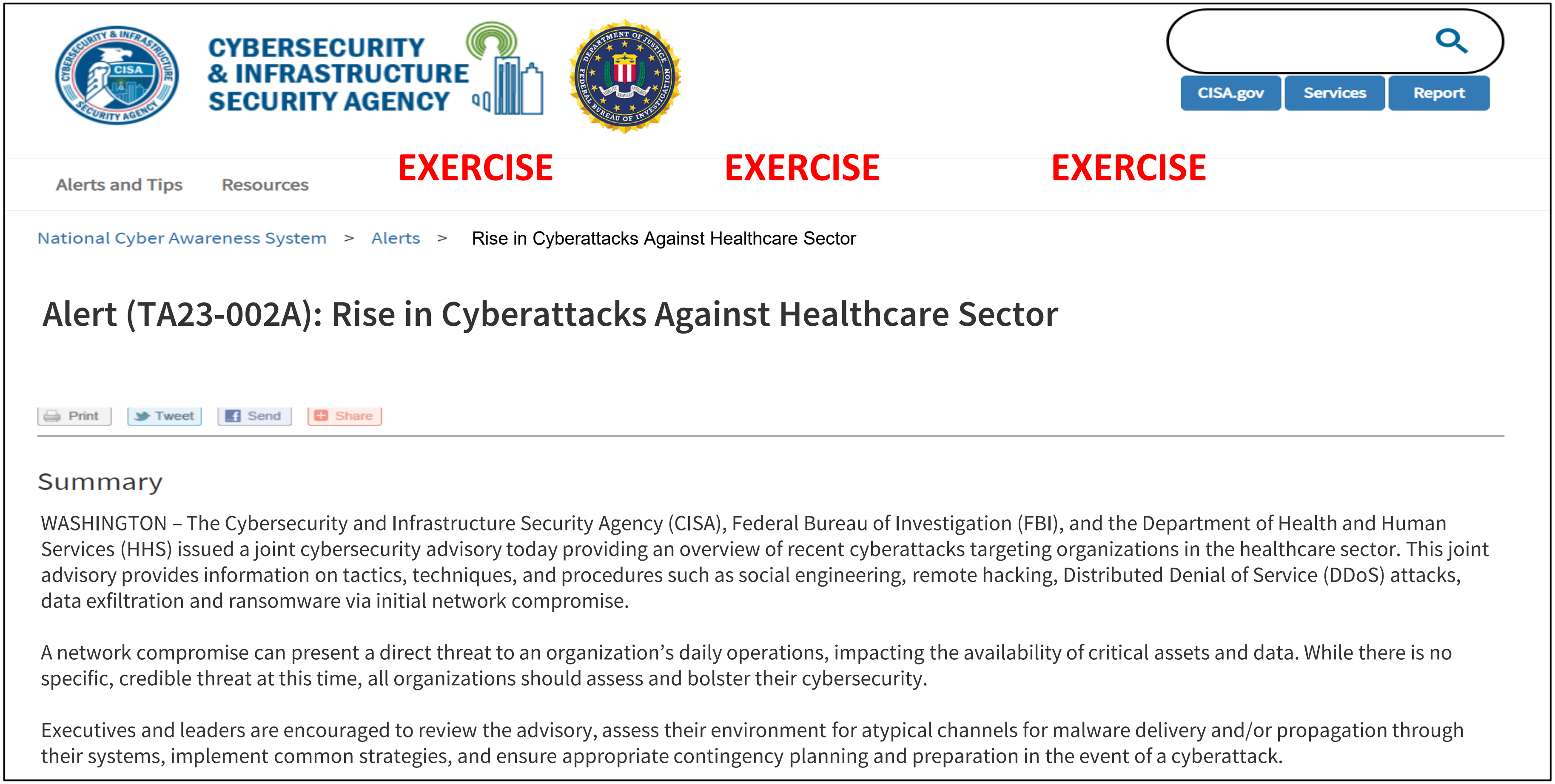
- **Players** have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
- **Observers** may support the development of player responses to the situation during the discussion 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.
- **Note-takers** document exercise discussions for the Summary Report.

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 used by cyber criminals, including phishing emails, ransomware, remote hacking, Distributed Denial of Service attacks (DDoS), and data exfiltration from healthcare organizations.



EXERCISE EXERCISE EXERCISE

National Cyber Awareness System > Alerts > Rise in Cyberattacks Against Healthcare Sector

Alert (TA23-002A): Rise in Cyberattacks Against Healthcare Sector

Summary

WASHINGTON – The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) issued a joint cybersecurity advisory today providing an overview of recent cyberattacks targeting organizations in the healthcare sector. This joint advisory provides information on tactics, techniques, and procedures such as social engineering, remote hacking, Distributed Denial of Service (DDoS) attacks, data exfiltration and ransomware via initial network compromise.

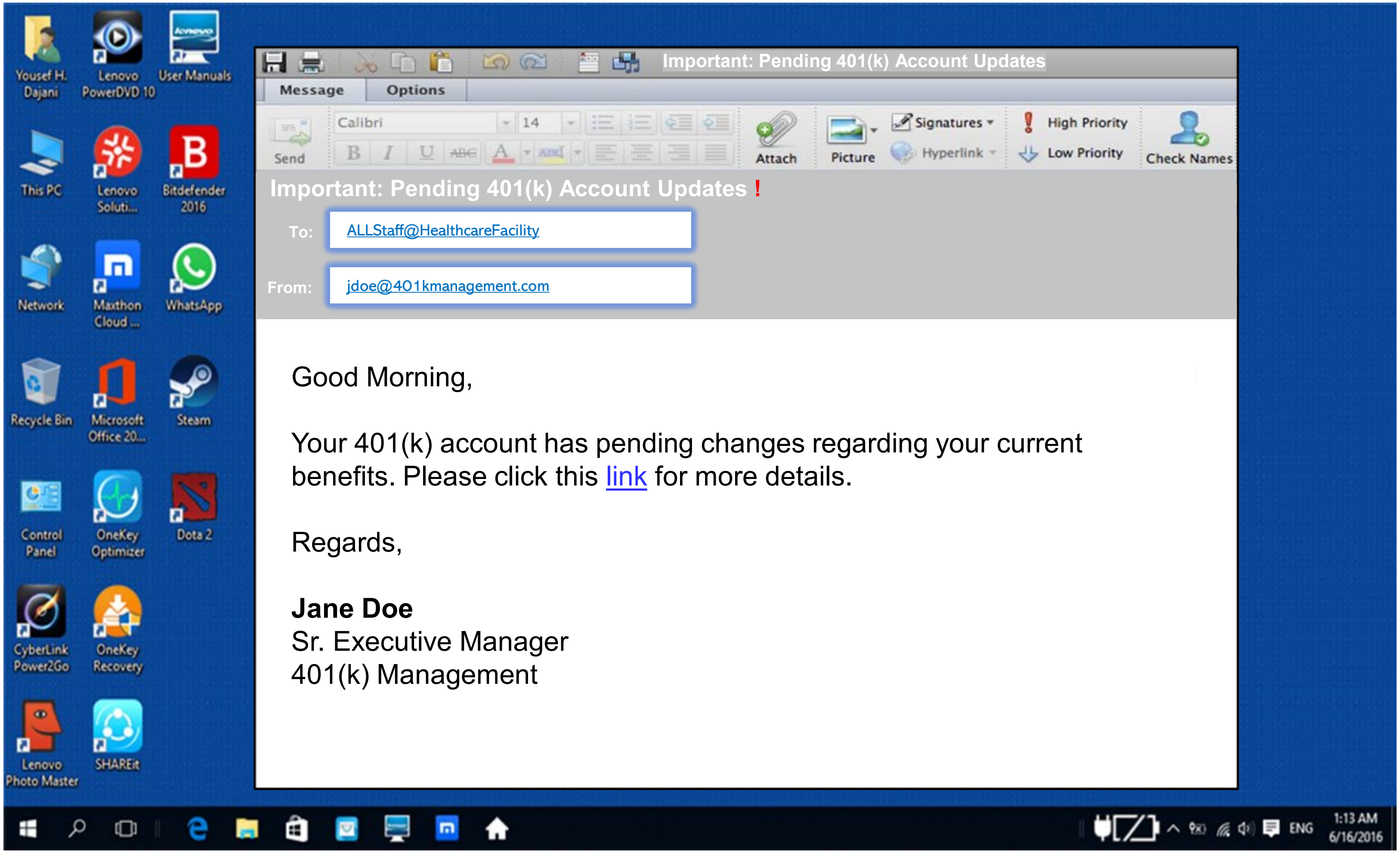
A network compromise can present a direct threat to an organization's daily operations, impacting the availability of critical assets and data. While there is no specific, credible threat at this time, all organizations should assess and bolster their cybersecurity.

Executives and leaders are encouraged to review the advisory, assess their environment for atypical channels for malware delivery and/or propagation through their systems, implement common strategies, and ensure appropriate contingency planning and preparation in the event of a cyberattack.

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 are unaware of any changes to the 401(k) and requests a copy of the email.



Important: Pending 401(k) Account Updates

Important: Pending 401(k) Account Updates !

To: ALLStaff@HealthcareFacility

From: jdoe@401kmanagement.com

Good Morning,

Your 401(k) account has pending changes regarding your current benefits. Please click this link for more details.

Regards,

Jane Doe
Sr. Executive Manager
401(k) Management

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.

MODULE 1 DISCUSSION

Discussion Questions

1. What is the greatest cybersecurity risk to your facility?

Discussion Questions

2. What cyber threat information 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?

Discussion Questions

3. What cybersecurity training does your facility provide your staff?
   a. How often must they complete this training?
   b. What happens if the training is not completed?
   c. Who is required to complete this training?

Discussion Questions

4. What essential functions depend on information technology, and what are the effects throughout the facility if they are disrupted?

Discussion Questions

5. How do employees report suspicious emails?

Discussion Questions

6. Describe your patch management and cybersecurity protocols for third-party technology vendors.
   a. How do vendors notify you that maintenance and updates are required?
   b. How do you communicate your cybersecurity concerns to your vendors?
   c. What cybersecurity language is included within your vendor contracts?

Discussion Questions

7. How regularly are users required to change their passwords?
   a. What is your account lockout policy if users don’t change their passwords in a timely fashion?
   b. What are the facility’s requirements for password length and level of complexity?

BREAK

Please complete the feedback form!

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

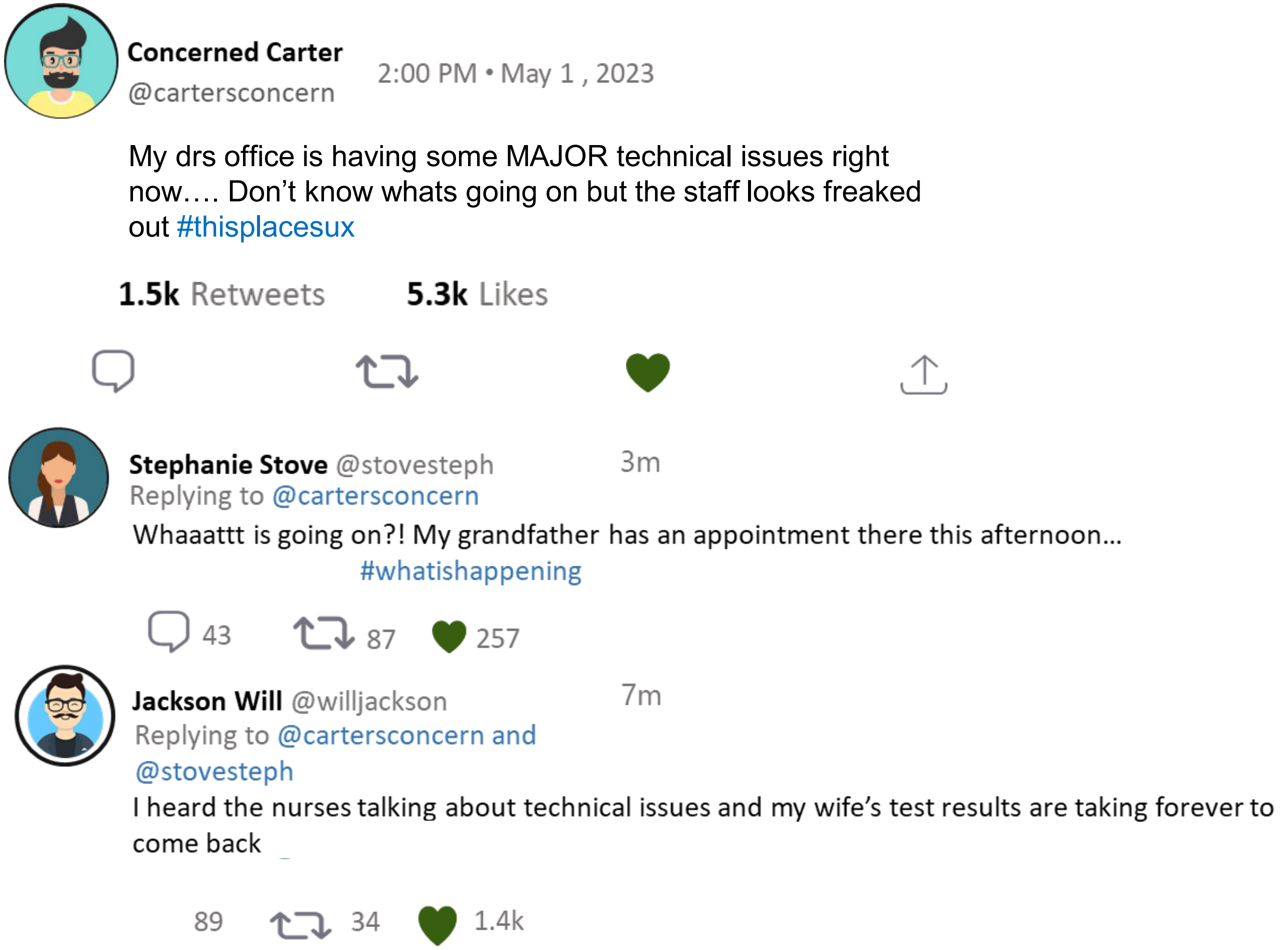
Nurses on the floor report that patient records are displaying incorrect information about medication, diagnoses, and personal information.

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.



Concerned Carter @cartersconcern 2:00 PM • May 1 , 2023

My drs office is having some MAJOR technical issues right now…. Don't know whats going on but the staff looks freaked out #thisplacesux

1.5k Retweets **5.3k** Likes

💬 🔁 ♥ ⤴

Stephanie Stove @stovesteph 3m
Replying to @cartersconcern
Whaaattt is going on?! My grandfather has an appointment there this afternoon… #whatishappening

💬 43 🔁 87 ♥ 257

Jackson Will @willjackson 7m
Replying to @cartersconcern and @stovesteph
I heard the nurses talking about technical issues and my wife's test results are taking forever to come back

89 🔁 34 ♥ 1.4k

MODULE 2 DISCUSSION

Discussion Questions

1. How would you rate the severity of these events?
    a. What are your priorities? What do you do first?

Discussion Questions

2. Describe the decision-making process for responding to a cyber incident.
   a. What options are available?
   b. What options are documented in plans?
   c. Do you have a response team you can activate?
      i. How are they activated?

Discussion Questions

3. What processes are used to contact critical personnel at any time, especially outside of business hours?

Discussion Questions

4. How does the facility proceed if critical personnel are unreachable or unavailable?

Discussion Questions

5. How are your electronic medical records (EMR), electronic health records (EHR), and business data backed up?

Discussion Questions

6. 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?
    b. At what point would they be initiated?

Discussion Questions

7. 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?

BREAK

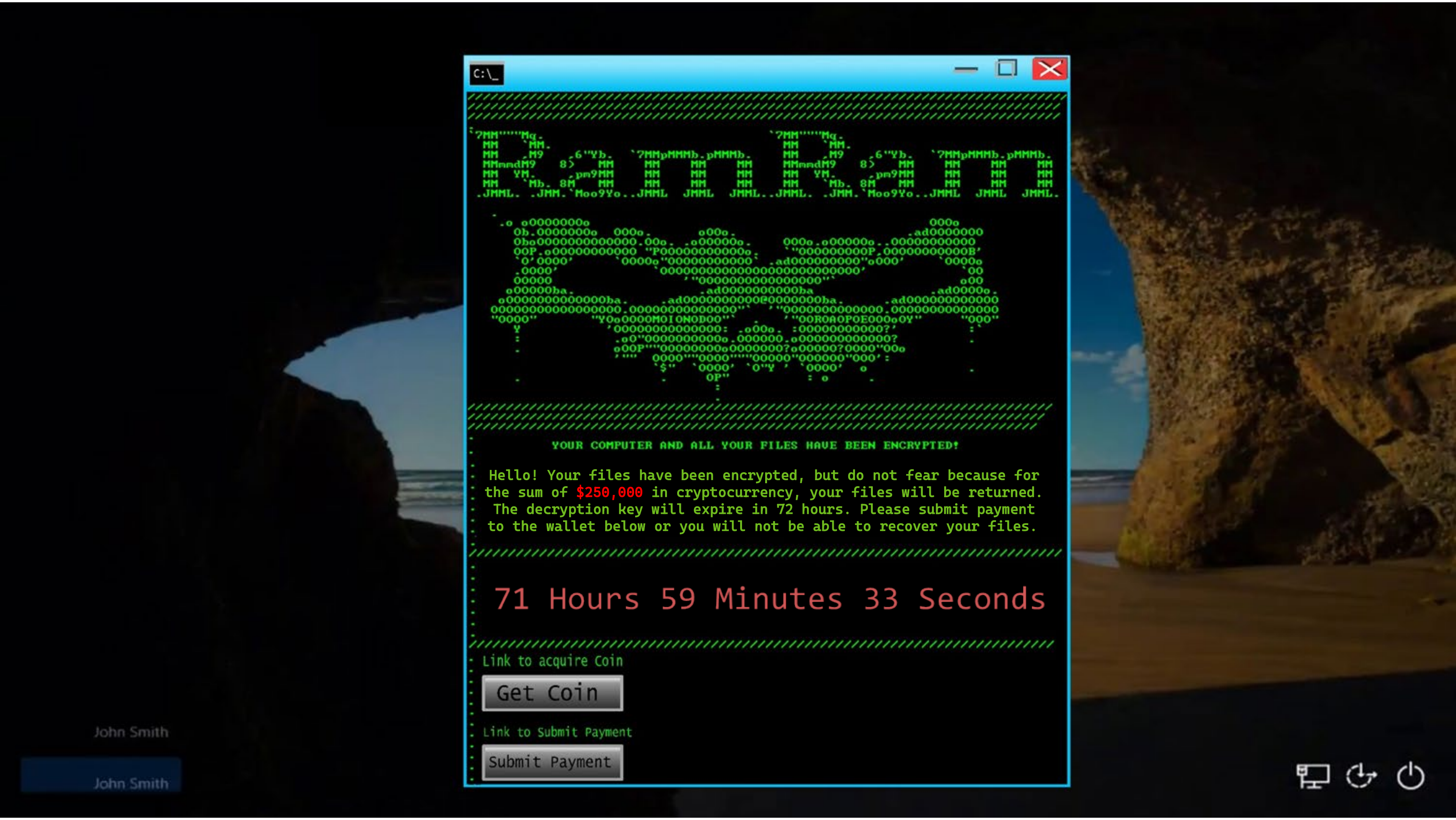
Please complete the feedback form!

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 $250,000 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.”



YOUR COMPUTER AND ALL YOUR FILES HAVE BEEN ENCRYPTED!

Hello! Your files have been encrypted, but do not fear because for the sum of $250,000 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.

71 Hours 59 Minutes 33 Seconds

Link to acquire Coin

Get Coin

Link to Submit Payment

Submit Payment

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.

MODULE 3 DISCUSSION

Discussion Questions

1. What is the decision-making process for responding to ransomware?
   a. What actions would be taken based on your incident response plan?
   b. Do you have a cyber insurance policy? What does it cover?
   c. What are the advantages/disadvantages to agreeing/refusing to pay?
   d. What are the potential legal and reputational ramifications?

Discussion Questions

2. 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?

Discussion Questions

3. At what point do you contact law enforcement during a cyber incident?

Discussion Questions

4. Where does your facility store backups of vital records? Are your backups stored in a location that is separated from your primary working copies of your files?
   a. How long do you keep 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 backup?

Discussion Questions

5. Who is responsible for public information dissemination related to the incident? What training or preparation have they received?
   a. Who would the public relations team contact in the event of an incident?
   b. How are these contacts prioritized?

Discussion Questions

6. What are your concerns with regards to these events impacting your facility’s reputation in the community?

HOTWASH

Hotwash

- Strengths
- Areas for Improvement
- Additional Comments

Please complete the feedback form!

CLOSING COMMENTS

Closing Comments

Nicole Coarsey

Division Manager, Healthcare Access

Well-Ahead Louisiana

WELL-AHEAD

WELLAHEADLA.COM

For more information:

CISA.gov

CEP@hq.dhs.gov

Questions?

Email:

kristin.lockwood@cisa.dhs.gov

Phone:

202-731-3451

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA