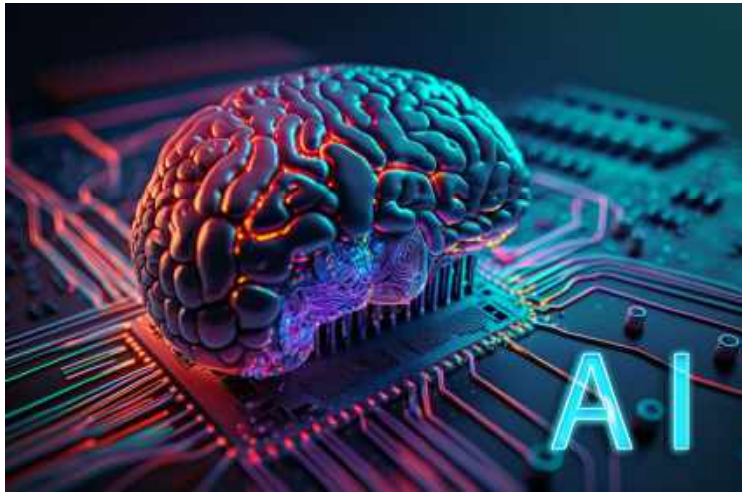
EXERCISE

AI/Cybersecurity Tabletop Exercise



Agenda

- Exercise Objectives
- Rules for the Exercise
- Scenario
- Modules (x3)
  - 1 – The Attempt
  - 2 – Oh No!
  - 3 – Let's Recover
- Exercise Review ("Hot Wash")

Exercise Objectives

EXERCISE

1. Validate the planning components established for an adverse event impacting cybersecurity/Information Technology systems.
2. Understand potential negative impacts AI can have and how they relate to your facility's cybersecurity preparedness posture.
3. Identify integration strategies for continuity of health care service delivery.
4. Identify opportunities for coordination during health care system recovery.
5. Discuss business continuity best practices and their effects on the recovery processes.

Rules for Players

- This is a **no-fault, low stress** exercise.
- Respond based on your current capability.
- Allow for **artificialities** of the scenario.
- Exercise participant safety takes priority over exercise events.
- Real-world emergencies take priority over exercise actions.
- For an emergency that requires assistance, use the phrase **"real-world emergency."**
- All exercise communications will begin and end with the statement **"This is an exercise."**
- **Avoid** sending exercise communications to organizations that are not aware of the exercise or are not actively participating.

Exercise Scenario

Cyber criminals are becoming increasingly sophisticated in their ability to obtain sensitive information from businesses, especially healthcare organizations.

Recently, several large corporations nationwide have been impacted, resulting in a **Level 5 Severity**.

This is defined as an emergency-level incident within the specified jurisdiction that poses an imminent threat to the provision of wide-scale critical infrastructure services; national, state, or local government security; or the lives of the country's, states, or local government's residents.

Module 1: The Attempt

Module 1: The Attempt

EXERCISE

April 11, 2024 **Time: 0900 hrs.**

Your Human Resource Director receives an email from what looks to be your facility administrator's account. However, it includes an unusual request for sensitive information, and you know your facility administrator is on vacation until tomorrow. Appropriately, your HR Director flags this as spam and ignores the email.

April 11, 2024 **Time: 1100 hrs.**

Later, the HR Director receives another email from the same email address. They are still requesting the sensitive information. The tone now is slightly more demanding and impatient. The new email also contains an invitation to connect via a Zoom video conference to verify their identity and authenticate the request. The HR Director accepts.

Module 1: The Attempt

EXERCISE

April 11, 2024 **Time: 1500 hrs.**

Both your HR Director and the "facility administrator" meet on Zoom to discuss the request. After being reassured during the video conference that the request is genuine your HR Director relents and provides the requested information, which includes user login credentials and passwords as well as financial account information. Following the release of information your HR Director tells you what happened.

Module #1: Key Issues

EXERCISE

- The HR Director has received an **unusual email** from what appeared to be the facility's administrator. Fortunately, the HR Director flagged it as **spam**.
- The HR Director has received another email requesting the same information. This time, however, the sender also includes a request to **verify their identify through Zoom**.
- Following a short discussion, which seemed to be a confirmation of the facility administrator's identity (validating the request) the **sensitive information was released** to the requestor.

Module #1: Discussion

EXERCISE

The Attempt: Discussion Points

EXERCISE

1. Having been told your HR Director released this information and knowing your admin is on vacation, do you take any action at this time?
2. Is there any other verification to ensure the person you are meeting on a Zoom call is who you want it to be?
3. Does your organization allow for sensitive information to be discussed via Zoom or other video conferencing?
4. Do you notify any external partners at this time such as the HCC, law enforcement, fusion center, or County EMA?
5. What specific training have your personnel received on identifying and mitigating potential cyber-attacks?
    - Are any of the trainings specific to AI-powered attacks such as machine learning techniques?

Module 2: Oh No!

Module 2: Oh No!

EXERCISE

April 12, 2024 Time: 0800 hrs.

Reports that systems are sluggish or frequently crashing are being submitted by users throughout the building this morning.

Your facility administrator has now returned and receives notice that large sums of money have been withdrawn from the organization's bank accounts.

A meeting is immediately convened with senior management, including the HR Director who reminds the Administrator of their Zoom call yesterday where they requested access information to the systems and financial accounts. The confused facility administrator informs the HR Director that at the time in question they were on a flight returning home from vacation.

Module 2: Oh No!

EXERCISE

April 18, 2024 Time: 1400 hrs.

The IT Department completes an investigation of the facility's computer systems. Their forensic analysis reveals that an attack has occurred and that it was perpetrated using a sophisticated AI-driven malware which was deployed to target both the facility's network and its banking information.

April 18, 2024 Time: 1600 hrs.

The facility administrator has received a message from the attackers which includes their demand for a large ransom payment in the form of cryptocurrency in exchange for restoring access to encrypted/inaccessible files and accounts.

Module 2: Key Issues

EXERCISE

- IT systems throughout the facility are running slower than normal and frequently crashing.
- You have identified that the HR Director did not meet with the real facility administrator.
  - Instead, a **sophisticated deepfake** was used as a method of social engineering.
  - System access and financial information was shared.
- IT staff have identified that you are the victim of a **complex AI-driven malware attack**.
- A **ransom demand** has been received. Cybercriminals have stated that it must be paid to restore your systems and banking.

Module #2: Discussion

EXERCISE

Oh No!: Discussion Points

EXERCISE

1. What are the incident priorities? What response actions are taking place?
2. Does your EOP address this type of situation?
3. What alternations to normal operations need to be conducted to maintain continuity of operations?
4. How would you decide whether to negotiate with the attackers or pursue alternate recovery options?
5. Do you have in-house IT or a business relationship with a third-party IT company or specialist?
6. How does your organization stay updated on the latest advancements in AI technology that could potentially be exploited by cyber threat actors?
7. In the event of a successful AI-powered cyberattack resulting in a data breach, what are the documented steps for conducting a thorough forensic analysis to identify the root cause and extent of the breach, as well as for determining the specific AI techniques or models employed by the attackers?
8. Do you know how to buy cryptocurrency?

Module 3: Let's Recover

Module 3: Let's Recover

EXERCISE

July 31, 2024 **Time: 0715 hrs.**

- Your incident response plan has been initiated and response operations have been underway.
  - The first critical steps taken were to isolate the affected systems and networks (containing the attack's spread).
  - All incoming internet traffic was blocked, and compromised devices were immediately disconnected.
  - Financial institutions were also contacted to report the breach.
- Your incident command center is established, with teams clearly designated for domains like operations, communications, legal, and more.
- Your facility has engaged a dedicated cybersecurity team and looped in third-party experts who specialize in AI-driven cyberattacks. As they begin their comprehensive analysis, you were able to quickly notify the relevant authorities, such as local and state law enforcement's cybercrime divisions, CISA, and other industry cybersecurity organizations.
- Preserving evidence is also paramount. You have taken steps to ensure all system logs, network traffic data, and other digital footprints left by the attack are securely stored for future forensic investigation.

Module 3: Let's Recover

EXERCISE

July 31, 2024 **Time: 0900 hrs.**

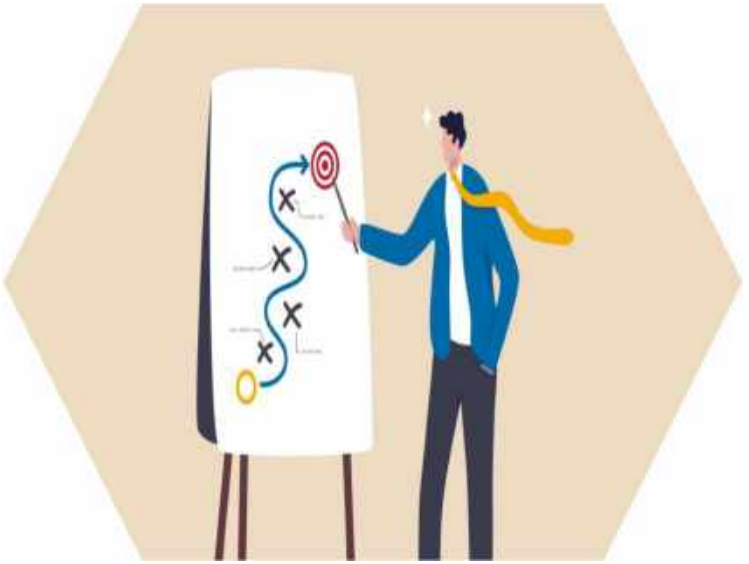
- With the assessment complete, your focus has now shifted largely from response to recovery.
- Uncompromised backup data has been restored, while affected systems are being rebuilt from the ground up with new hardened security controls and defensive AI technologies to prevent similar attacks.
- A substantial backlog of paper charting and other documentation, resulting from an extended period of downtime procedures, is still being deciphered and uploaded as systems become available.
- You have stood up and continue to maintain systems allowing for transparent communications - both internally to employees and externally to partners, patients, customers, and regulatory bodies.

Finally, a thorough post-incident review is conducted, breaking down every aspect of how this AI-driven attack transpired. The findings reveal gaps in your AI and cybersecurity posture that will need to be addressed through updated processes, increased AI literacy training for personnel, and continuous monitoring for emerging AI-based threats.

Module 3: Key Issues

EXERCISE

- Relying on your EOP and activated incident command center, response actions have been underway for some time enabling the **quarantine of impacted systems**.
- There is a **significant amount of data needing to be entered** to account for the prolonged period of downtime operations.
- A detailed and **comprehensive analysis** has been completed by a dedicated cybersecurity team specializing in AI-driven attack.
- A thorough **post-incident review** is being conducted which has identified gaps in your organization's cybersecurity posture and awareness of AI-generated threats.



Module #3: Discussion

EXERCISE

Let's Recover: Discussion Points

EXERCISE

1. What are the priorities for a successful recovery?
2. Does your facility have a comprehensive recovery plan that pertains to Information Technology (IT) systems failures and/or significant interruptions?
3. What are your workarounds?
4. Have you completed a business impact analysis?
5. Who is responsible for uploading paper chart information into new systems?
6. Do you have cyber insurance?
   - If yes, what does it cover? Lawsuits, ransom, response charges incurred
   - Who do you go to in order to enact it? IT, HR, Admin?
7. Does your Continuity of Operations Plan (COOP) include downtime procedures and alternate strategies for patient charting, accounts receivable, accounts payable, and providing payroll during an IT disruption or failure?
8. Due to the long-term downtime how will the manual entry of paper charting be entered into the electronic systems? Who will do it?

Exercise Hot Wash

AI / Cyber Security: Hot Wash

EXERCISE

- What have you learned during the exercise?
- Name three (3) of your organizational strengths
- Name three (3) of your organizational weaknesses/gaps
- What should the next steps in planning and preparing be?
- List and prioritize three (3) ***short-term*** and three (3) ***long-term*** actions that you would like to address in the future

EXERCISE

AI/Cybersecurity Tabletop Exercise

COMPLETE