2024 Health-ISAC Discussion Based Exercise Series After-Action Report

2024 Exercise Conduct

This exercise series was generously sponsored by:

ACALVIO AI-POWERED DECEPTION
Akamai
ARMIS
CELERIUM
digicert
ISSQUARED
netskope
proofpoint.

Executive Summary

From March to November 2024, Health-ISAC held ten workshops as part of the Discussion Based Exercise Series, involving over 100 member organizations, potential members, and strategic partners. Each three-hour exercise focused on a ransomware scenario, with participants discussing updates and sharing best practices, experiences, and recommendations. The exercises aimed to explore opportunities for enhancing security and resilience in the health sector. Variations in the scenarios and discussions catered to the diverse participants, encouraging active engagement. Observations from these exercises have been compiled into the following categories to guide continuous improvement in cybersecurity and preparedness, ultimately fostering greater resilience in the health sector.

- Employee Training and Awareness
- Credential and Network Vulnerability Mitigation
- Attack Vectors and Mitigation Strategies
- Ransom Payment
- Intelligence and Outreach
- Scope of Breach
- Legal and Public Affairs
- Release of ePHI Data
- Public Confidence
- Chain of Custody
- Law Enforcement
- Strategies for Resiliency

This report provides a brief summary of the full *2024 Health-ISAC Discussion Based Exercise Series After-Action Report (AAR)* that Health-ISAC members received on February 6, 2025. Health-ISAC members can retrieve the full report in the Health-ISAC Threat Intelligence Portal (HTIP).

Exercise Overview

Exercise Name	**Health-ISAC Discussion Based Exercise Series**
Scope	This discussion-based exercise engaged participants in facilitated discussions to exchange ideas and capture processes used by Health-ISAC member organizations and partners.
Objectives	This exercise series provides a forum for Health-ISAC members and potential members to use a focused security scenario to prompt discussions and to share approaches from leaders in the community regarding security preparedness and resiliency and discuss issues, concerns, best practices, lessons learned, and other points to help inform preparedness, response, and resiliency activities.
Scenario	A large urban hospital system (a Health-ISAC member) is a leader in restoration services to patients suffering from trauma, cancer, burns, and deformities. An Advanced Persistent Threat-Actor (APT) has been actively performing reconnaissance of the U.S. Healthcare sector and has discovered weaknesses in the hospital's network environment. This results in phishing aimed at deploying malware and acquiring credentials.
Exercise Sponsors	The exercise was developed and facilitated by Health-ISAC with additional sponsorship from Acalvio, Akamai, Armis, Celerium, Digicert, ISSQUARED, Netscope, and Proofpoint.

Scenario Summary

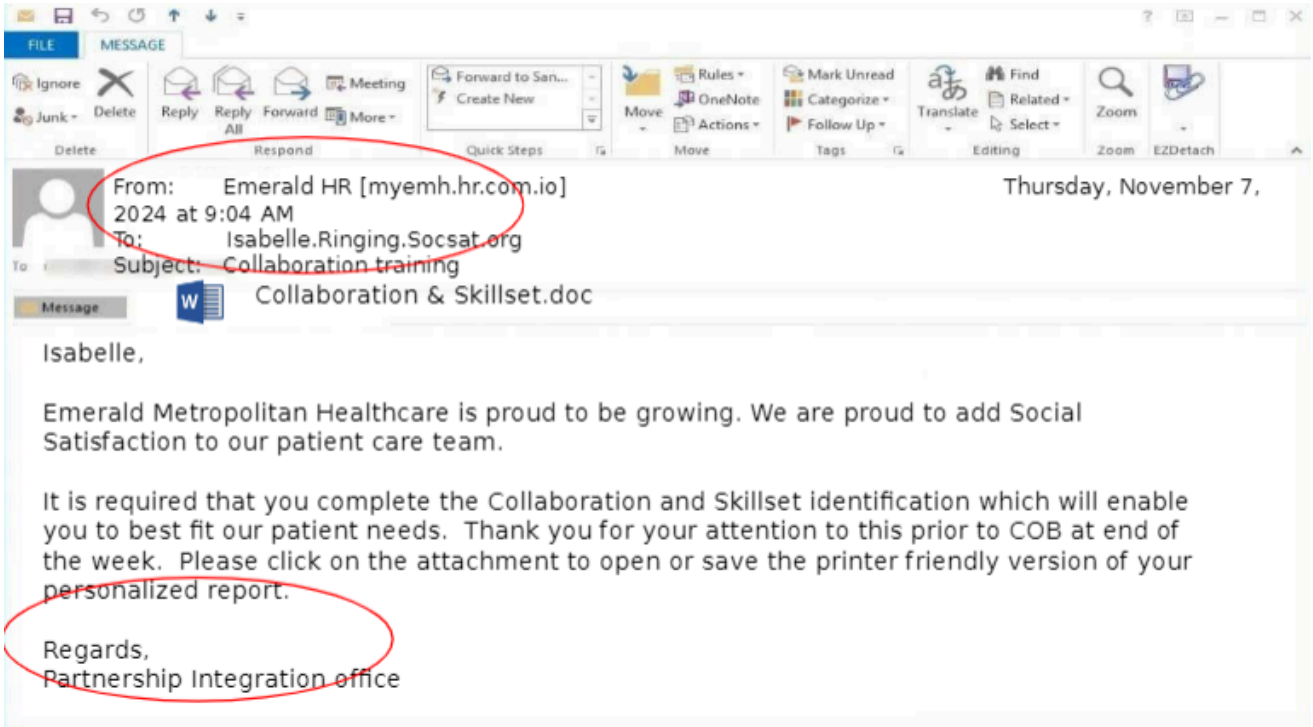
Situation Update (Fictional Ground Truth)

- **Emerald Metropolitan Healthcare (EMH)** is a large urban hospital system and a Health-ISAC member.
- After expansion - EMH now leads in offering restoration services to patients suffering from trauma, cancer, burns, and deformities.
- Techniques to restore the functionality and appearance of patients improve the quality of life.

Module 1

Inject 1

- An Advanced Persistent Threat-Actor (APT) has been actively performing reconnaissance of the U.S. Health Sector and has discovered weaknesses in Emerald's network environment.
- A Phishing campaign has proved successful aimed at deploying malware and acquiring credentials.



Inject 2

- Ransomware messages appear on various computer stations.
- Message includes Tor download instructions to pay.
- RFIs to Health-ISAC infer origination from the Bluecat group - Russian criminal RaaS variant.
- Extent of exfiltration (if any) unknown.
- Several critical functions in the reconstructive surgery and burn center have been affected.
- With outreach, recovery of these critical functions performed as decryption keys were validated and used.
- Forensic discovery for exfiltration continues.

Inject 3

- Several critical functions in the reconstructive surgery and burn center have been affected.
- With outreach, recovery of these critical functions performed as decryption keys were validated and used.
- Forensics discovery for exfiltration continues.

Module 2

Inject 1

- Following refusal to pay, hospital administration has been contacted by numerous angry patients who state someone has their medical records and will post embarrassing personal photos and information if the patient does not pay.
- Per admin, fees seem to range from a few hundred to a thousand dollars each.
- Patients demand to know why these records are released and threaten legal action.

Inject 2

- Cybercriminals utilized open-source information, such as social media accounts, to “enhance” harvested Electronic Protected Health Information (ePHI) data to leverage victims.
- Attackers exert pressure on victims by sharing sensitive photos with family, friends, and colleagues - even creating public-facing websites to embarrass and harass.
- Indications are that over 50,000 patients in various attacks nationwide are targeted – elevating criminality.

Observations

This section provides a summary of key observations from ten exercises. The summary is based on feedback from participants, planners, and debrief sessions, reflecting various perspectives on exercise execution and scenario-related insights. These observations are intended to guide discussions on continuous improvement actions within the organization.

Where directive or absolute terms such as “must” or “should” are used, that is to capture the general consensus of the conversation from a given workshop (or workshops) and does not necessarily reflect the position of Health-ISAC and should not be taken as a directive statement. **A brief summary of the observations is included below as ideas for organizations to consider as they strive to bolster their preparedness and resilience.**

Employee Training and Awareness

The human factor is a key vulnerability in cybersecurity, emphasizing the need for continuous training to combat threats like phishing. Organizations typically conduct annual compliance training, monthly simulations, and gamified activities such as phishing tournaments to maintain engagement without overwhelming employees. Customized training for specific roles, like C-suite executives, addresses unique risks. Rewards, rather than penalties, encourage participation and improvement. Platforms like KnowBe4 and Mimecast support simulations, and metrics like phishing report rates assess program success. Regular campaigns and standardized tests help track progress, ensuring organizations maintain a culture of security awareness and continuous improvement across all employees, including contractors.

Credential and Network Vulnerability Mitigation

Participants emphasized the need for strong cybersecurity measures to address credential threats and network vulnerabilities. Key strategies included Multi-Factor Authentication (MFA), Single Sign-On (SSO), and Zero Trust models, alongside the "least privilege" principle. Password security was enhanced through longer requirements, password managers, and secure reset protocols.

Endpoint and network protection were strengthened with sandbox isolation and strict software installation policies. Phishing defenses like safe attachment scans, email banners, and AI-powered detection were vital. Communication platforms like Health-ISAC's Threat Intelligence Portal were valued for timely threat intelligence sharing. Proactive measures, such as executive advocacy for stronger vendor contracts, were also stressed.

Attack Vectors / Mitigation Strategies

Phishing remains a primary vector for ransomware, but new attack methods, like AI-driven voice and text phishing, are emerging. Insider threats, both intentional and accidental, pose significant risks, with mitigation strategies including access restrictions, employee support, and monitoring departing staff. Virtual Private Network (VPN) vulnerabilities, MFA failures, and weak authentication practices are also targets, necessitating strong identity management and passwordless authentication. Data loss prevention requires tools like Netskope, network segmentation, and tight control over remote access and bring-your-own-device (BYOD) policies. Third-party risks can be minimized through rigorous vendor security measures. Employee training and monitoring tools are critical for defending against social engineering attacks.

Ransom Payment

Deciding whether to pay a ransom is complex, with most organizations defaulting against payment while considering legal, financial, operational, and ethical factors. Legal concerns include compliance with regulations like Office of Foreign Assets Control (OFAC) and Office for Civil Rights (OCR), and potential fines. Operationally, payment may speed recovery but doesn't guarantee success, as decryption tools may fail. Financially, insurance plays a role in negotiation, but contracts should be reviewed ahead of time. Reputation risks include incentivizing future attacks. Key decision factors include breach severity, data exfiltration proof, and recovery options. Establishing relationships with legal, insurance, and law enforcement, along with solid backup strategies, is critical for effective response.

Intelligence and Outreach

Effective incident response requires coordination across legal, operational, and strategic areas. Legal teams ensure compliance with regulations, manage external communications, and protect privileged information. Cyber insurance considerations include notification obligations and coverage limitations. Adhering to regulatory reporting, like CIRCIA's 72-hour rule, and maintaining relationships with law enforcement and regulatory bodies is vital. Trusted partners, such as forensic and backup teams, help maintain operations. Health-ISAC provides a platform for sharing threat intelligence and collaborating with peers. Incident response plans (IRPs) should include pre-established contacts and regular updates to improve preparedness. Transparent communication with stakeholders and customers is essential for managing crisis impacts.

Identifying Scope of Breach

Identifying the scope of a data breach requires collaboration between internal teams and external experts, utilizing thorough log audits, forensic investigation, and effective incident response. Participants highlighted the importance of reviewing network logs, ensuring visibility across systems, and comparing traffic against baseline patterns. Third-party partners, such as incident response (IR) retainers, can aid in investigations, legal coordination, and notifications. Advanced tools, like AI forensic modeling and CTI, help detect anomalies and identify threat actors' tactics. Engagement with agencies like CISA and the FBI enhances threat intelligence. Preparedness through regular IRP testing and maintaining detailed records strengthens future breach response and recovery efforts.

Legal and Public Affairs

Participants emphasized the critical role of legal and public affairs teams in incident response, stressing the need for proactive communication strategies and integration into IRPs. Legal teams manage cyber insurance, forensics, law enforcement engagement, and oversee communications to protect attorney-client privilege. They also handle privacy concerns, particularly with Protected Health Information (PHI) or Personally Identifiable Information (PII), and ensure compliance with regulations. Public affairs teams must manage transparent, empathetic messaging, avoiding premature statements or misinformation. Predefined messaging templates, coordination with employees, and effective patient communication are key. Regular tabletop exercises and employee education ensure readiness, foster collaboration, and prevent miscommunication during crises.

Release of ePHI Data

Participants discussed the challenges of managing response and recovery during the release of sensitive data, such as ePHI. Key considerations include dark web monitoring, which helps track leaked data to prevent follow-up attacks and protect consumer trust. Effective recovery requires assessing data integrity and confidentiality, understanding affected data, and leveraging trusted partners like forensic teams. Crisis management coordination is essential, with both technical teams focused on recovery and leadership handling external pressures. Clear crisis communication plans, including pre-approved messaging, are vital. Reputation management, regulatory compliance, and regular exercises also play crucial roles in effective response and recovery strategies.

Public Confidence

Participants emphasized strategies for maintaining public confidence during cyber events, particularly in healthcare, where reputational damage can have lasting effects. Proactive messaging is key to controlling the narrative, with careful wording and continuous updates from response teams. Legal teams must balance transparency with legal restrictions, sharing only permissible information. Public confidence is measured by stock price, patient volume, and retention. A crisis communication plan, including a designated spokesperson and call tree, is essential for consistent messaging. Internal notification is crucial, with clear guidance for staff to control the narrative, especially on social media. Security certifications and robust controls are also vital for trust.

Chain of Custody

Participants discussed the importance of maintaining a proper chain of custody during cyber incidents, involving collaboration between legal, forensic, and operational teams. Pre-incident planning, including protocols for evidence collection and third-party vendor engagement, is crucial. Forensic teams, often external, play a key role in maintaining evidence integrity. Legal counsel oversees compliance with laws and ensures defensible actions in court. The scope of the breach affects evidence collection, especially in remote work environments. Remote forensics require tools like Endpoint Detection and Response (EDR) systems, though risks of data loss remain. Organizations may need to collaborate with law enforcement or third-party experts for efficient evidence handling and resource management.

Law Enforcement

Participants highlighted the complexities of law enforcement involvement in incident response, focusing on preparedness and coordination. While law enforcement expertise can aid recovery, their engagement may introduce delays, especially in high-profile cases. Concerns include potential data loss during server confiscation, though the FBI typically ensures evidence preservation. Law enforcement's focus on prosecution may conflict with an organization's recovery goals. Proactive planning and pre-established relationships with law enforcement and third-party partners help streamline responses. Legal oversight, including compliance with the Cybersecurity Information Sharing Act, is critical for managing risks and ensuring effective collaboration, especially with off-premises infrastructure and remote evidence collection.

Strategies for Resiliency

Participants emphasized strategies to enhance organizational resilience, focusing on communication, collaboration, and investment in cybersecurity. Key recommendations included implementing a comprehensive communication strategy to prevent misinformation and regular updates to stakeholders. Proactive engagement with government agencies like CISA and local law enforcement was encouraged, along with education for executives on cybersecurity threats. Regular tabletop exercises (TTXs) involving internal and external teams help improve coordination and preparedness. Data protection strategies, such as onsite backups and post-quantum encryption, were advised to secure critical assets. Vendor contracts should include cybersecurity stipulations, and organizations must continuously monitor regulatory compliance to ensure adherence.

APPENDIX A: ACRONYMS

AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat-Actor
BEC	Business Email Compromise
BYOD	Bring-Your-Own-Device
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act of 2022
CISA	Cybersecurity and Infrastructure Security Agency
EDR	Endpoint Detection and Response
EMH	Emerald Metropolitan Healthcare
ePHI	Electronic Protected Health Information
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
GETS	Government Emergency Telecommunications Service
Health-ISAC	Health Information Sharing and Analysis Center
HIPAA	Health Insurance Portability and Accountability Act
HPH	Healthcare and Public Health
HTIP	Health-ISAC Threat Intelligence Portal
IOC	Indicators of Compromise
IR	Incident Response
IRP	Incident Response Plan
IT	Information technology
MFA	Multi-Factor Authentication
MSP	Managed Service Providers
NCSC	National Cyber Security Centre
OCR	Office for Civil Rights
OFAC	Office of Foreign Assets
PHI	Protected Health Information
PII	Personally Identifiable Information
RaaS	Ransomware as a Service
RACI	Responsible, Accountable, Consulted, and Informed
RFI	Request for Information
ROI	Return on Investment
SAS	Spectrum Access System
SEC	Securities and Exchange Commission
SIM	Security Information Management
SLA	Service Level Agreement
SSO	Single Sign-On
TTP	Tactics, Techniques, and Procedures
TTX	Tabletop Exercise
VPN	Virtual Private Network
WPS	Wireless Priority Service